Security Controls on Scientific Information and the Conduct of Scientific Research

A White Paper of the Commission on Scientific Communication and National Security

Homeland Security Program
Center for Strategic and International Studies

June 2005

CONTENTS

Statement of the problem

In the 21st century, neither geographical isolation, agricultural productivity, natural resources, nor military manpower can suffice to "provide for the common defense, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity." Scientific and technological accomplishments – and a workforce trained to exploit them – are necessary to defend the nation and enhance its quality of life.

However, know-how that is generated in the course of scientific research is available to anyone participating in that research. If the results of that research are published openly, they become available to all—including to those who may seek to use those results maliciously. Therefore, policies to limit the ability of terrorists to access and exploit scientific research may gain approval which have the effect of constraining participation in, and dissemination of, that research.

Such limitations do not come without cost. Open communication and participation are fundamental to the conduct of high-quality research, so constraints on that openness can have serious repercussions for the quality of that research, for the health of research and educational institutions, and ultimately for the societal objectives that research and education serve: national and homeland security, economic prosperity, health, environmental protection, and quality of life. Moreover, given the global nature of the scientific and technical enterprise, unilateral national policies to control scientific and technical information may have little prospect of effectively doing so. Information controls should not be imposed unless they can be shown to be effective and worth the penalties that they impose.

Current U.S. government policy

It has been the policy of the United States since the Truman Administration that fundamental scientific research should be conducted without government restrictions on participation by researchers or publication of results unless a formal process has led to a determination that access to the work should be limited, for specific national security reasons, to individuals with the proper security clearances – in other words, that the research has been classified. Current U.S government policy is set out in National Security Decision Directive 189 (NSDD-189), issued in the Reagan Administration, which provides that "to the maximum extent possible, the products of fundamental research remain unrestricted."[1] This directive recognized, as had its predecessors, that the United States' "leadership position in science and technology is an essential element in our economic and physical security," and that "the strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component." Accordingly, the Directive specifies that "where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and

[1] National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical, and Engineering Information," September 21, 1985.

engineering at colleges, universities and laboratories is classification." It goes on to direct that to the extent consistent with U.S. Statutes, "no restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification."

The Directive has remained in effect through subsequent Administrations, and it was explicitly reaffirmed as recently as November 1, 2001 by Dr. Condoleezza Rice, then Assistant to the President for National Security Affairs. Dr. Rice confirmed in a letter to Dr. Harold Brown, co-chairman of the CSIS Council on the Future of Technology and Public Policy, that "the policy on the transfer of scientific, technical, and engineering information set forth in NSDD-189 shall remain in effect, and we will ensure that this policy is followed."

This Directive does not assert that the open dissemination of unclassified research is without risk. Rather, it says that openness in research is so important to our own security – and to other key national objectives – that it warrants the risk that our adversaries may benefit from scientific openness as well. And even though today's adversaries differ from the ones we faced during the Cold War, the world's scientific and technological landscape has also evolved. Science and technology are global enterprises, and our ability to constrain their adverse application by unilaterally restricting their dissemination is if anything even poorer today than it was when NSDD-189 was issued.

Recommendations with respect to current U.S. government policy

- *The Commission recommends that NSDD-189, reflecting policy that has been in effect in generally the same terms since the Truman Administration, should continue to be the central principle governing security controls over fundamental research. NSDD-189 makes a strong statement about openness in the conduct and dissemination of unclassified fundamental research and represents a careful balance between the needs of research institutions and the requirements of national security.*

- *The Commission recommends further that NSDD-189 be implemented carefully with an eye to avoiding incursions on openness. This paper examines the administration of current U.S. policy and makes recommendations with respect to current and proposed implementation of information control mechanisms.*

The underlying issue: the importance of openness

When research and education are not free to draw on the world's brightest minds, to invite any and all to critique and validate research results, and to foster the dynamic and often serendipitous interactions from which successive innovations can arise, excellence will suffer. Practices that limit the open interchange of ideas or open participation in research and educational activities – in other words, policies that compartmentalize ideas, findings, or research approaches and limit their access to certain categories of student or researcher – will limit the effectiveness of our research and educational system, impairing its ability to serve national needs.

Open participation. Scientific talent is distributed worldwide, without regard to national borders. Laboratories that hope to compete at the top of their fields must therefore be free to recruit the brightest researchers, wherever they may be found. Excellence is self-perpetuating: top-quality research institutions recruit and retain professional staff by offering the chance to work with the best students and junior researchers – who, in turn, seek to join those institutions where the most exciting research is already underway. Arbitrary limitations on who can attend a school, join a laboratory, or participate in a research project may cut off contributions from valuable potential participants. Limits on participation in research activities are particularly problematic for research universities, whose research and educational missions are interdependent, and which are physically ill-prepared and philosophically unwilling to segregate facilities or discriminate on the basis of national origin. Institutions that cannot – or that are not allowed to – engage the best prospective students and researchers will be unable to remain competitive in a dynamic global environment that offers these individuals many alternatives.

The United States no longer holds a monopoly on scientific preeminence in today's highly competitive and thoroughly globalized research environment; there are first-rate laboratories all over the world. By imposing unnecessary barriers on the research activities of U.S. institutions, an overly zealous or inflexible export control system will make it impossible for U.S. researchers to keep abreast of technical activity conducted outside the United States, and the United States will necessarily fall behind. Given the importance of science and technology to national security and economic well-being, such restrictions on the United States research enterprise threaten to put this nation's security and quality of life at risk.

Open communication. The progress of science depends on independent review and validation of research results by all who are able to judge the work's quality, assess its significance, and build upon it. These reviews take place through a variety of formal and informal mechanisms – conversations within a laboratory; presentations at professional meetings; informal circulation of a manuscript prior to submission to a publisher; formal peer reviews of manuscripts as part of the publication process; and validation and verification of work by subsequent investigators after research has been published. Moreover, science is cumulative. Research results can make possible future advances only if those results are known to others.

Limiting the dissemination of research necessarily constrains the ability of independent experts to verify or extend it. Attempts can be made to circulate results within a restricted community, or in some cases on a classified basis. However, history is replete with examples of research for which the most significant applications have been made by individuals whose contribution could never have been predicted in advance, and who would never have been included in a restricted list of reviewers. Limiting dissemination of results restricts the opportunity for such interaction. Moreover, limiting the detail with which experimental procedures are specified similarly impedes the ability of independent researchers to validate the work, precluding the acceptance of those results as scientific findings and imperiling their ability to underpin future research.

Caveats. Note that advantages of openness, as weighed against the risks of transfer to dangerous recipients, may differ for fundamental research (activity motivated by the quest for understanding, the results of which typically have diverse, diffuse, or indeterminate application) as compared to technology development (activity intended to solve specific problems, the applications of which can be more directly envisioned, at least initially). Indeed, NSDD-189 refers specifically only to the former, implying that the case for controls is stronger for the latter. However, the distinction between "fundamental research" and "technology development" is not necessarily clear – or even, in some cases, meaningful. Many fundamental scientific advances have been closely associated with applications. Instead of considering the quest for understanding and the quest for application as opposite ends of a one-dimensional continuum, they can be considered to lie along perpendicular axes that divide the space of scientific and technical activity into four quadrants. One of these quadrants represents work that is both fundamental and motivated by application – as exemplified by Louis Pasteur, whose microbiological research was motivated both by the desire to understand disease processes at a very fundamental level and by the desire to cure those diseases.[2] Therefore, for the purposes of applying NSDD-189, the fact that research may be motivated by a particular application should not imply that it cannot be "fundamental."

Mechanisms to control conduct and dissemination of research

Five principal mechanisms have been considered for limiting the conduct and dissemination of research and development in situations when open participation and communication is thought to be contrary to the national interest. They all have a role for some types of scientific and technical activity, but not all are appropriate for fundamental research:

- classification on national security grounds denies access to anyone without a government-issued security clearance and a demonstrated "need-to-know" the information;
- export controls regulate the transfer of certain information (and possibly access to certain equipment) to foreign nationals and therefore constrain who can participate in associated research and educational activities;
- some provisions in federal research contracts can specify results to be "sensitive but unclassified," restrict publication, or provide for advance government review or approval of who can perform the research;
- statutes control the conduct of certain types of research; and
- self-governance by the scientific community restricts, or requires advance review of, research proposals or publications.

[2] "Donald Stokes, "Completing the Bush Model: Pasteur's Quadrant," talk given at a conference "Science: The Endless Frontier 1945 – 1995;" December 9, 1994; available online at http://cspo.org/products/conferences/bush/Stokes.pdf (last accessed May 27, 2005). See also Donald Stokes, *Pasteur's Quadrant : Basic Science and Technological Innovation* (Washington, DC: Brookings Institution, Press 1997).

1. Classification

The most stringent national security restriction that can be put on scientific and technical information is classification. With rare exceptions, only information that is owned by, produced by or for, or is under the control of the U.S. government is eligible to be classified.[3] Only designated government officials have the authority to classify information, and classification decisions are supposed to be made in accordance with guidelines that specify the damage that might result if that information were made public.[4]

Current U.S. classification policy explicitly provides that "scientific, technological, or economic matters relating to the national security" can be classified, but that policy goes on to state that "basic scientific research information not clearly related to the national security shall not be classified."[5] Security classification makes little sense for information that can readily be derived independently; after all, withholding the results of a given experiment does not destroy the underlying reality, which remains available to be rediscovered by others. In some cases, such as when experimental capabilities are limited by technical barriers that are suddenly lifted with the development of new tools, many researchers may be in a position to perform a given experiment, and classification of some such work would do little to constrain the rest. In other cases, however researchers with unique equipment, novel experimental approaches, clear vision, or simply serendipity may obtain research results that would not likely soon be independently repeated. Even in these cases, research results may be sufficiently distant from application (beneficial or malicious) that classification would also be inappropriate.

In those areas of research where classification might be appropriate – for example, where "government-supported research demonstrably will lead to military products in a short time," to quote a landmark 1982 National Academy of Sciences report[6]– it will come at a cost. Most universities do not conduct classified research on campus because the associated constraints are incompatible with their educational mission,[7] although several have associated off-campus research facilities that perform classified research. Moreover, only individuals who have been issued security clearances by the government

---

[3] The exceptions are certain categories of nuclear-weapons related information, which are considered "born secret" under the Atomic Energy Act no matter how they were generated, and secrecy orders that can be imposed by the government on patent applications under the Invention Secrecy Act.

[4] Executive Order 13292, issued on March 25, 2003, establishes Bush Administration policy on the classification of national security information.

[5] E.O. 13292, sections 1.4(e); 1.7(b)

[6] Panel on Scientific Communication and National Security, Committee on Science, Engineering, and Public Policy, *Scientific Communication and National Security* (Washington, DC: National Academy Press, 1982), p. 5; available online at http://www.nap.edu/books/0309033322/html/ (last accessed May 27, 2005).

[7] In 2002, the Massachusetts Institute of Technology reviewed and reaffirmed its policies against classified research on campus. See *In the Public Interest: Report of the Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information*, Massachusetts Institute of Technology, June 12, 2002. http://web.mit.edu/faculty/reports/publicinterest.pdf (last accessed May 27, 2005).

are permitted access to classified work. Therefore, security classification limits both the institutions and the personnel who are in a position to contribute to research activities.

When government agencies sponsoring technical activity believe that the results of that activity will need to be reviewed for possible security classification, they have the responsibility to conduct that activity in institutions that are appropriately equipped to handle classified information. Technical activity not conducted in such institutions would presumably not be expected to raise classification questions. However, most government grants for unclassified technical activity specify that if the grantee believes the results of that work warrant classification, the grantee has the responsibility to limit the dissemination of that work and to contact the appropriate U.S. government agency that would have the authority to classify it. In such extraordinary cases, the initiative to seek classification rests with the grantee, not the government.

Recommendations with respect to classification

- *The Commission recommends that classification remain the mechanism by which research results requiring national security protection be controlled. Procedures involving the classification and declassification of information are well-defined, and in principle, they can be consistently applied in ways that take the costs and the benefits of controls into account.*

- *The Commission concurs with existing policy that fundamental scientific research that is not clearly relevant to national security remain unclassified.*

- *The Commission recognizes the responsibility of researchers doing nominally unclassified research to call their results to the attention of the relevant government agencies in the extraordinary event that they believe those results to warrant classification.*

2. "Deemed Export" Controls

At present, the United States regulates the export of defense-related goods and services as well as the export of "dual-use" goods and services that have legitimate civilian use but that can also assist the proliferation of weapons of mass destruction, facilitate terrorism, or interfere with important U.S. foreign policy objectives. Controls on defense-related goods and services are administered by the State Department's Directorate of Defense Trade Controls and on dual-use goods and services by the Commerce Department's Bureau of Industry and Security. Corporations, individuals, or other entities seeking to export such items must apply to the government for an export license, and those shipping controlled items out of the country without a license risk civil and criminal penalties.

Both the State Department and the Commerce Department control systems regulate the export of *information* that pertains to controlled goods or services. Exports include not only shipping controlled goods, services, or information out of the country, but also conveying them or otherwise making them available to foreign nationals within the United States. Such transactions are "deemed" to be exports, and they similarly require

export licenses. Export license applications are evaluated on the basis of the particular goods, services, or information to be exported and the identity of the prospective recipient.

Proposed extensions of export controls. Consistent with NSDD-189, the export control regulations of both the State Department and the Commerce Department exempt fundamental research from controls so long as the research is "ordinarily published and shared broadly within/in the scientific community."[8] However, despite the fact that NSDD-189 also states that the "conduct" of unclassified, federally funded, fundamental research should not be restricted, except as provided in U.S. statutes, these export control regulations do not explicitly address whether licenses may be required for access to export-controlled equipment that is used in the conduct of fundamental research. In practice, research universities have acted as if licenses were not required.

Certain specialized areas of fundamental research, however, are affected by the more stringent State Department munitions controls. For example, scientific research satellites are explicitly treated as a military, and not a dual-use, technology for export control purposes. Therefore, universities conducting space-based research have had to obtain export licenses from the State Department before allowing certain foreign researchers to work on aspects of those projects. Although the universities agreed they needed to comply with legal obligations, they found export control requirements in these cases difficult to reconcile with university policies requiring open participation and open publication, as well as with NSDD-189. Responding to Congressional direction,[9] the White House (beginning in the Clinton Administration and continuing into the Bush Administration) worked with the State Department to review its regulations and relax their impact on these university space-based research programs. As a result, the State Department amended its export control regulations in March 2002 and narrowed somewhat – but did not eliminate – the set of countries for which licenses would be required to have their citizens participate in this research.[10]

The assumption that the fundamental research exemption broadly covered at least those areas of research that did not fall under State Department controls was challenged by a series of reports issued in early 2004. Every year, as required by law, a set of federal agency Inspectors General (IGs) prepares a coordinated set of reports on some aspect of

---

[8] Export Administration Regulations, Part 734.8(a) (using "within") and International Traffic in Arms Regulations (22 CFR Ch. 1 section 120.11(8) (using "in")

[9] The conference report for the FY 2000 Appropriation Bill for the Departments of Veterans Affairs and Housing and Urban Development, and for Sundry Independent Agencies, Boards, Commissions, Corporations, and Offices for the Fiscal Year Ending September 30, 2001 (House Report 106-988) found that recent legislative changes had had the unintended byproduct of subjecting university-based fundamental research programs to "overly restrictive and inconsistent ITAR [International Traffic in Arms Regulations] direction." This report directed the White House Office of Science and Technology Policy "to work jointly with the National Security Council, in consultation with the NASA Administrator and the Secretary of State, to expeditiously issue clarification of ITAR that ensures that university collaborations and personnel exchanges, which are vital to the continued success of federally-funded research, are allowed to continue as they had under the long-standing fundamental research exception in the Export Administration Regulations."

[10] The Federal Register, Vol. 67, no. 61, March 29, 2002, pp. 15099-15101.

export controls. The 2003 reports included compliance by research institutions and universities. The Commerce Department IG's report[11] contained several recommendations which, if accepted by the Commerce Department, could severely limit the fundamental research exemption.

The report included a section titled "BIS [Commerce Department Bureau of Industry and Security, which implements dual-use export controls] Regulations and Policies Could Enable Foreign Nationals from Countries and Entities of Concern to Access Otherwise Controlled Technology,"[12] which repeated findings from earlier Commerce Department Inspector General reports. Although no evidence was presented that any security breaches had resulted, this section questioned (either explicitly or implicitly) whether a number of existing export control exemptions were overly broad, permitting foreign nationals from "countries and entities of concern" to access "otherwise controlled technology." However, the report also noted that BIS could not address these exemptions by itself, and no specific recommendations on these points were made. Specifically mentioned in this section were:

- Exempting from control work "intended" for publication, which would permit access to research that might not in fact be published (possibly because of security concerns that led the researcher to forego publication) and questioning whether intent to publish alone was a sufficient determinant of whether research should fall under the fundamental research exemption;
- Exempting from control educational information conveyed through "catalog courses and associated teaching laboratories of academic institutions"; and
- Exempting from control information conveyed to foreign nationals with permanent resident status.

The report went on to raise security concerns that had not been addressed in the earlier reports, and it recommended dealing with these concerns by tightening deemed export regulations in two ways:

- Broadening the conditions under which the use of controlled technology by foreign nationals would require an export license, and informing research institutions that deemed export controls would apply in such circumstances "even if the research being conducted with that equipment is fundamental," [13] and
- Requiring that export licenses be obtained for foreign nationals on the basis of their country of birth, regardless of their country of citizenship.[14]

---

[11] U.S. Department of Commerce, Office of the Inspector General, "Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the U.S.," Final Inspection Report No. IPE-16176, March 2004 (http://www.oig.doc.gov/oig/reports/2004/BIS-IPE-16176-03-2004.pdf ; last accessed May 27, 2005).
[12] Ibid., pp. 10-13
[13] Ibid., pp. 15
[14] "Foreign nationals" in this context do not include permanent residents or citizens of the United States or members of certain legally protected categories such as asylum seekers.

The first of these recommendations could have the effect of significantly narrowing the fundamental research exemption, and it is discussed in greater detail below. The second recommendation would not expand the set of controlled activities, but it could increase the number of people doing already-controlled activities for which licenses would be necessary. To the extent that fundamental research remains exempt from deemed export controls, the second recommendation does not affect it.

Inconsistency with NSDD-189. The Inspector General's report contains only a passing reference to NSDD-189, and that discussion deals only with the *results* of fundamental research; it makes no mention of the Directive's parallel discussion of the *conduct* of such research. Perhaps for this reason, the IG report does not address the apparent inconsistency between its recommendation to expand deemed export controls and NSDD-189's direction that "no restrictions may be placed upon the conduct … of [unclassified] federally-funded fundamental research."[15] Admittedly, the same inconsistency can be found in the position of the Commerce Department's Bureau of Industry and Security, which according to the IG report asserts that "technology relating to controlled equipment … is subject to the deemed export provisions *even if the research being conducted with that equipment is fundamental*."[16] Nevertheless, the Bush Administration's reaffirmation of NSDD-189 can be interpreted to mean that deemed export controls should not be applied at all to fundamental research, much less expanded.

Difficulty of administering "use" controls in fundamental research. Beyond – or perhaps because of – their inconsistency with NSDD-189, the changes recommended by the Inspector General regarding access to or use of controlled equipment could have serious implications for fundamental research undertaken at academic institutions.[17]

1. Ambiguity of controls. From a practical point of view, it may be very difficult to determine, from the export control regulations themselves, exactly which pieces of laboratory equipment would be subject to licensing, and at what point exposure to or use of controlled technology would constitute a transfer of knowledge sufficient to be deemed an export requiring an export license.[18] The Commerce Control List (which specifies those dual-use items for which export is controlled) is hundreds of pages long and far from clear, and tremendous effort on the part of

[15] The qualifying language "except as provided in applicable U.S. Statutes" that follows the quoted language in NSDD-189 does not change this conclusion. Deemed export controls are provided in regulation, not in statute.
[16] U.S. Department of Commerce, Office of the Inspector General, *op cit.,* footnote 11 above, p. 15 (emphasis added).
[17] See July 30, 2004 letter of from Alice Gast, MIT Vice President for Research, and 11 other senior university research officials, to Undersecretary of Commerce Kenneth I. Juster; see also September 9, 2004 letter from MIT President Charles Vest and 21 other university presidents to senior White House officials.
[18] The Commerce Department has requested public comment on how the revisions in deemed export regulation proposed by the Inspector General would affect research-performing institutions in the United States, and in particular is requesting information on the number of foreign nationals who would require licenses and the impact of compliance with new licensing requirements. *Federal Register*, March 28, 2005 (Volume 70, Number 58), pp. 15607-15609; Docket No. 050316075-5075-01

universities may be required to ascertain what, if any, equipment or material available in university labs is subject to export controls.

2. Discrimination on the basis of nationality. Export license requirements depend on the nationality of the recipient. These controls involve singling out individual students, scholars, or researchers who would not be able to have access to equipment (although their work would be entirely unclassified) that others working on the same research would be able to use.[19] Just as in the case of the current "no fly lists," there potentially may be serious difficulties involved in singling out individuals, especially in certain cultures where many names may be identical. Moreover, many leading research universities have made it clear that they have neither the human resources nor the will to selectively segregate their research facilities in this fashion.

3. Difficulty in controlling access. Because scientific equipment can be shared by several laboratories or moved from one to another, an institution could not readily determine which students and researchers would require licenses to work in which laboratories. Moreover, depending on the degree of exposure to controlled equipment that is warranted to require a license, physical controls may have to be installed to prevent unlicensed individuals from accessing laboratories with such equipment. In many cases, such equipment is in use—or, at least, accessible for use—24 hours a day, meaning that access would have to be controlled on a "24/7" basis.

4. Lack of Timeliness and Inflexibility. Given the length of time needed to secure export licenses and the fluid and unpredictable nature both of university research programs and of laboratory equipment purchases, timely license processing for foreign students and scholars will be difficult to achieve. Without sufficient lead time, the probability increases that foreign nationals will either be turned away when they apply or will be deterred from applying to work in the United States in the first place.

Adverse aspects of "use" controls in fundamental research. In addition to practical implementation difficulties, there are other important adverse aspects of a control regime that holds out the prospect of requiring license applications for foreign students and scholars in research and educational institutions.

1. The security benefits are modest. United States export controls have no effect on constraining the access of adversaries to technology that is available from uncontrolled sources *outside* the United States. In today's globalized scientific and technical enterprise, United States universities and research institutions compete for talent against equivalent institutions all over the world. To remain competitive, many of these foreign institutions procure sophisticated experimental equipment on world markets and develop advanced instrumentation domestically.

[19] Technology transferred in catalog courses of instruction is exempt from controls, but information and technology transfers in the process of conducting research could constitute export-controlled transactions.

However, few of them are required by their own governments to limit the participation of non-citizens in state-of-the-art research.[20] Foreign students and researchers who consider coming to United States have an ever-widening array of alternative options outside the United States that are not subject to U.S. deemed export controls. Therefore, unless U.S. controls are restricted to the use of technologies that are truly unavailable outside the United States or other countries with equivalent levels of control, they provide little or no security benefit, and will serve only to damage the U.S. research enterprise.

Moreover, the operation, maintenance, installation, and even repair of controlled equipment do not convey the ability to reproduce that equipment in another setting—after all, auto dealers cannot make cars. Acquiring the equipment itself from the United States would require a license, providing a layer of protection that is independent of controls on the technical knowledge.

2. Important discoveries may be hindered. The rapid and dynamic nature of state-of-the-art research makes it hard to predict exactly the disciplines in which a researcher will work; the colleagues or labs he or she will join or collaborate with; the equipment to which he or she may require access; and the modifications which may have to be made to that equipment. Licensing requirements, and their concomitant delays, can eliminate the spontaneous discoveries that arise from serendipitous interactions and spur-of-the-moment collaborations. During a conversation or a seminar, a researcher may realize that his or her laboratory apparatus is well-configured to solve a colleague's problem. If export licenses are required to use that apparatus, or even to share technical exchanges about the possible application, the opportunity may be lost.

3. Research talent may be lost. The mere possibility that certain researchers may necessitate export licenses will introduce delays and uncertainties that may discourage the best foreign researchers from coming to the United States (i.e., the so-called "chilling effect")—researchers from whom this country not only benefits, but upon whom we increasingly depend to maintain our scientific and technical base.[21] Such licensing requirements will also force universities and research institutions to discriminate among their students or staff on the basis of characteristics other than academic merit, skills, and expertise – a further disincentive to foreign researchers that is inconsistent not only with many publicly stated institutional policies but also with a number of principles and policies fundamental to the US polity.

---

[20] France, Russia, and the United Kingdom are the only major research powers that have anything like a "deemed export" regime.

[21] The dependence of the United States science and technology base on foreign-born scientists and engineers has been extensively documented. One of the most recent studies on this topic is The National Academies, *Policy Implications of International Graduate Students and Postdoctoral Scholars in the United States* (Washington, DC: The National Academies Press, 2005), available online at http://books.nap.edu/catalog/11289.html (last accessed May 31, 2005). See statistics listed on p. 1.

4. Contact with the leading edge of science may be reduced. Inhibiting foreign interchange, in turn, inhibits the ability of U.S. researchers to stay abreast of scientific and technological developments outside this country. There is also the possibility that other governments may seek to retaliate in some fashion.

An alternate approach. Despite the inappropriateness of imposing an overall deemed export control regime on the conduct of fundamental research, it may nevertheless be appropriate for the government to require that deemed export licenses be obtained for transfers of technology to specifically identified individuals *if specific adverse information exists about that individual*. U.S. export control regulations already contain a feature that provides the authority to prevent any U.S. entities from assisting foreign programs or entities that are developing weapons of mass destruction, regardless of whether that assistance otherwise violates export control regulations and regardless of whether that assistance can be obtained elsewhere. This feature is in the form of a requirement to apply for an export license—which would then be denied—for any transaction that the seller knows, or has reason to know, is destined for a foreign WMD program. If the U.S. government has information revealing that a pending sale is intended for use in a WMD program, it can inform the seller of that fact, thereby triggering the licensing requirement. Such an approach cannot be assured of depriving the target WMD program of those goods or assistance, which may be available from suppliers outside the scope of U.S. controls, or may be indigenously developed. (Note that embargoing U.S. technologies related to nuclear weapons from North Korea has not prevented that country from developing nuclear weapons.) However it does serve a political objective of "keeping U.S. hands clean," and it may complicate the WMD weapons programs' procurement activities.

Such an "individually targeted" provision might be used if the U.S. government needed a mechanism to exclude specific individuals who are known to be affiliated with proscribed foreign activities or institutions (e.g., affiliated with WMD programs or with hostile intelligence agencies) from accessing certain technologies or gaining certain scientific or technical "know how." However, this situation should rarely come to pass. If the United States had such information, it would likely be used in visa and border reviews to deny such an individual entry to the United States. Nevertheless, if such an individual were admitted anyway, or if adverse information were obtained later that did not rise to the level of warranting expulsion, this option would provide a basis for denying that individual access to certain technologies without having to establish a licensing regime for an entire university campus that would target individuals on the basis of broad categorizations such as nationality or employer. Note that the existing Student and Exchange Visitor Information System indicates each foreign student or exchange visitor's host institution, and if the government wanted to establish this level of control for a specific visitor, it would be able to notify that host institution accordingly.

Recommendations with respect to export controls

- *The Commission recommends that, consistent with NSDD-189, no general "deemed export" controls be placed on the use of research equipment in the conduct of fundamental research at U.S. universities and research institutions.*

- *The Commerce Department IG's proposed threshold – which would require an export license for any one of the following activities: operation, installation, maintenance, repair, overhaul, **or** refurbishing" of commercially available equipment – is neither practical nor required to protect U.S. interests.*

- *In exceptional cases where the government possesses adverse information about a specific foreign national, but the information does not warrant that individual's expulsion from the country, the Commission recommends that the government have the option to notify that individuals' host institution that a deemed export license may be required before that individual is given access to certain technologies.*

- *The Commission recommends that the State Department and Commerce Department work closely with members of the academic and research community before making any changes to regulations governing deemed exports associated with fundamental research. Sustained engagement will be required for any control system to be both effective and to minimize adverse impact on U.S. research institutions.*

3. Federal Research Contract Provisions

Both governmental and industrial sponsors have proposed for inclusion in research contracts with academic research institutions clauses that would curtail openness in fundamental research. The Association of American Universities (AAU) and the Council on Governmental Relations (COGR), key associations of research universities, conducted a study in 2003 of the frequency with which such clauses were introduced.[22] This study explored two types of provision – one that gives the government rights of prior review of proposed research publications, and another that gives the government the authority to restrict the participation of foreign nationals in particular research projects. Both types of provision are harmful to fundamental research institutions for the reasons discussed above.

These provisions appear to be based on the self-protective instincts of lower level contracting officials rather than on articulated national policy. These provisions, when applied to fundamental research outside the context of classification, are not consistent with NSDD 189. Although some universities have accepted these clauses, several others have sought to negotiate them out of the contracts. These negotiations often succeeded with government agencies, but negotiating with industrial contracting offices was harder. Even though the specific work that industrial sponsors were seeking at universities might have qualified as fundamental research were the government to have contracted for it directly, industrial sponsors apparently believed that they were required to pass on restrictions that were imposed on their own prime contracts.

[22] A Report of the AAU/COGR Task Force "Restrictions on Research Awards: Troublesome Clauses," Julie T. Norris, Chair; Massachusetts Institute of Technology; http://www.aau.edu/research/Rpt4.8.04.pdf (last accessed May 27, 2005)

The AAU/COGR study pointed out that most research institutions have policies precluding research contracts that restrict publication rights. It also found that a lesser number, but still a majority, of research institutions refuse to restrict the participation of foreign nationals in campus research. In addition to the direct consequences of constraining university openness, the imposition of a requirement for pre-publication security review by the sponsor means that the resulting research is no longer considered to be intended for open publication, and that it therefore no longer qualifies for the fundamental research exemption. Therefore, imposing a pre-publication security review requirement can mean that export licenses will be required for foreign nationals participating in that research.

Recommendations with respect to federal research contract provisions

- *The Commission recommends that NSDD-189's proscription of restrictions on either the conduct or the reporting of unclassified fundamental research be respected, and that no requirements for pre-publication review of research or for approval of foreign nationals be included in government contracts involving fundamental research.*

- *The Commission recommends that the same policy "flow down" to institutions that perform fundamental research for the government as subcontractors. That is, if industrial prime contractors subcontract for fundamental research, they should not pass down to their subcontractors any pre-publication review requirements or approval authorities over foreign nationals that may derive from non-fundamental research provisions in their own contracts.*

4. Statutory requirements for the conduct of specific types of biological research

Legislation implemented in the wake of the 9/11 attacks imposed licensing and access control requirements on institutions that possess certain pathogenic organisms. The USA PATRIOT Act (2001) and the Public Health Security and Bioterrorism Preparedness and Response Act (2002) establish criteria that must be met by anyone with access to certain dangerous biological organisms, denoted as "select biological agents," and that require the Attorney General to certify whether individuals meet those criteria. Among other criteria, no citizen of a country designated by the Secretary of State as state sponsor of terrorism may have access to these organisms. Research institutions have had to implement access control procedures that exclude all uncertified personnel from areas where they might gain access to these agents.

When these access restrictions were being considered by Congress, the researchers most affected by them – microbiologists – supported them, agreeing that "some people should not have access to select agents." [23] Although the subsequent regulations have forced changes in laboratory design and operation and imposed costs and delays, universities and other research institutions have for the most part managed to implement them. As of

[23] See testimony by Ronald M. Atlas, Ph.D., President-Elect of the American Society for Microbiology and Co-chair of the Task Force on Biological Weapons Control, before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, November 6, 2001, available online at http://www.asm.org/Policy/index.asp?bid=5463 (last accessed May 27, 2005)

December 2004, 9,350 personnel have been cleared by the U.S. government to work with, or have access to or control over, these agents.[24]

Implementing select agent restrictions, however, should not be taken as a precedent for the research community's ability to implement a much more general "deemed export" regime as described in section 2 of this White Paper. Both the list of controlled items (agents), and the set of criteria specifying who is allowed access to them, is far more objective and specific for select biological agents than it appears they would be for export-controlled technologies. Moreover, whether or not a researcher will require access to controlled materials is likely to be far more predictable in the case of biological organisms than in the case of restrictions on export-controlled research hardware.

Controls on access to select agents are imposed by statute and therefore the policy in NSDD-189 does not apply.[25] However, there is concern, and some anecdotal information, that these restrictions may drive experienced researchers and laboratories out of select agent research.[26] At the same time, a large influx of research funding in select agent research is drawing researchers into the field. The long-term implications of these regulations on the field, including the effects of these inflows and outflows on research quality, are not yet known.

Recommendations with respect to legislative controls

- *The Commission recommends that the consideration of any proposed legislation that would impose controls on the transfer of scientific information be informed by the testimony at hearings by universities and research institutions, and that executive branch implementation of any such legislation be accomplished by government agencies working closely with members of the academic and research community. Sustained engagement will be required for any control system to be both effective and to minimize adverse impact on U.S. research institutions.*

- *The Commission recommends that the select agent control system not be considered as a precedent for a regime to govern access to export-controlled technologies.*

5. Self-regulation

Self regulation by the academic community is an effective way to achieve the government's underlying security goals. In the case of information generated in the

[24] Personal communication, Janet Shoemaker, Director of Public Affairs of the American Society for Microbiology, April 18, 2005

[25] The operative language of NSDD-189 prohibits restrictions on the conduct or reporting of federally-funded unclassified fundamental research "except as provided in applicable U.S. Statutes."

[26] Even with the more predictable, objective, and limited nature of select agent controls as opposed to other mechanisms to restrict unclassified research, an MIT faculty committee concluded that select biological agent controls "are not consistent with MIT's principles." The Committee expressed concern that at some future time, MIT may legitimately decide that research subject to these controls "is no longer in its interest. MIT Ad Hoc Faculty Committee on Access to and Disclosure of Scientific Information, *op cit.*, footnote 7 above, p. iii.

course of fundamental biological research, a group of scientific publishers, editors, scientists, and policy analysis recognized that "there is information that, although we cannot now capture it with lists or definitions, presents enough risk of use by terrorists that it should not be published."[27] Indeed, exactly what information falls in this category still eludes definition. Consistent with NSDD-189, the journal editors rejected a formal government role in making this determination – but in return, they assumed part of this burden themselves. Their statement of February 2003 pointed out that "an editor may conclude that the potential harm of publication outweighs the potential societal benefits," and that "under such circumstances, the paper should be modified, or not be published."[28] This responsibility is also shared, of course, by the researchers themselves.

While this statement was being drafted, a panel of the National Academy of Sciences (NAS) was meeting to come up with ways to minimize the risk that advanced fundamental biological research would be misapplied to create novel, and ever more dangerous, biological weapons. This panel's final report, named the Fink Report after the study chair, Gerald Fink, ultimately emphasized the importance of self-governance, individual responsibility, and institutional review in exercising security responsibilities.[29] In addition to reaffirming the journal editors' statement with respect to scientific publishing, the NAS panel went on to recommend that a screening process be established through which local review committees, operating under nationally derived guidance, would review proposals to conduct research in any of seven "areas of concern."[30] These reviews would seek to identify and mitigate issues that might arise from the research.

The federal government, in turn, has moved to implement the NAS panel's recommendations by establishing a National Science Advisory Board for Biosecurity (NSABB). According to its charter,[31] this Board will work with the scientific community to establish the voluntary screening process recommended by the NAS panel for certain categories of dual-use life sciences research. It also has the following responsibilities:

- Raise the awareness of scientists with respect to the security implications of their work;
- Help develop of a code of conduct for life sciences researchers;

---

[27] "Statement on Scientific Publication and National Security," Journal Editors and Authors Group, *Science* vol. 299, 21 February 2003, p. 1149. Available online at http://www.sciencemag.org/feature/data/security/statement.pdf (last accessed May 27, 2005).

[28] Ibid.

[29] Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, Development, Security, and Cooperation, National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academy Press, 2004). Available online at http://books.nap.edu/catalog/10827.html (last accessed May 27, 2005).

[30] These areas include research that would demonstrate how to render a vaccine ineffective; confer resistance to therapeutically useful antibiotics or antiviral agents; enhance the virulence of a pathogen or render a nonpathogen virulent; increase transmissibility of a pathogen; alter the host range of a pathogen; enable the evasion of diagnostic/detection modalities; or enable the weaponization of a biological agent or toxin. *Ibid*, p. 5

[31] At www.biosecurityboard.gov (last accessed May 27, 2005). As of the same date, the Board's membership had not been announced.

- Recommend education and training programs in biosecurity;
- Advise on policy concerning the publication, communication, and dissemination of "dual-use" biological research; and
- Recommend strategies for coordinated international oversight of dual-use research.[32]

As of this writing, the NSABB had still not been empanelled, although its first meeting has been scheduled for June 30-July 1, 2005.

Concerns about the security sensitivity of unclassified fundamental scientific research are particularly salient in the life sciences, but they are not limited to that field. Similar issues have risen, for example, in the area of critical infrastructure protection. In one recent example, a graduate student at George Mason University, near Washington, DC, assembled public domain and publicly available information to derive a fine-grained, geospatial database that mapped out the nation's critical infrastructures. National and homeland security officials expressed alarm that the resulting product, which could be used as a targeting tool, was not classified; however, because it was a privately generated compilation of public domain information, it was not eligible for classification.[33] Recognizing the security sensitivities involved – and working closely with government officials – the student, his faculty research advisor, and university officials agreed that the actual database would be very tightly controlled, and that any published version would speak in only the most general terms about the underlying database.[34]

Recommendations with respect to self-regulation

- *The Commission recommends that the NSABB be empanelled promptly so that it can carry out its assigned mission.*

- *The Commission recommends that each university and research institution establish a committee or other group made up of senior scholars that is responsible for informing faculty and researchers and promoting understanding with respect to classification, export controls, federal research contract provisions, statutory requirements on information control, and self-regulation. This entity would regularly assess compliance with same. By doing a better job at understanding their obligations to comply with export control legislation, universities will help to avoid government decisions that could hurt national interests more than they help. Innovative mechanisms to educate faculty, administrators, and general counsels as to their export control compliance responsibilities must be developed, particularly if the recommendation above to forego the use of deemed export controls to regulate the conduct of fundamental research is not adopted.*

---

[32] *Ibid*., NSABB Charter, March 4, 2004

[33] Laura Blumenfeld, "Dissertation Could Be Security Threat; Student's Maps Illustrate Concerns About Public Information," *The Washington Post*, July 8, 2003, p. A1

[34] "George Mason University at Forefront of Homeland Security Efforts and Developing Models of Public and Private Cooperation," *The CIP Report*, vol. 2, No. 3," July 2003, pp. 7-8 http://techcenter.gmu.edu/programs/cipp/cip_report/cip_report_2.1.pdf (last accessed May 27, 2005).

- *The Commission commends actions taken by members of the life sciences and critical infrastructure protection communities, among others, to consider the security implications of their own work and to take responsibility to implement self-governance mechanisms. Further thought and analysis are needed to formulate procedures regarding the dissemination of scientific information in these contentious areas; and to raise the education and awareness of practitioners. As one example, the existing requirement for National Institutes of Health-supported graduate students to have some training in ethics could provide a mechanism for this purpose.*

- *The Commission recommends that individual researchers pay careful attention to their responsibility, while doing nominally unclassified research, to call their results to the attention of the relevant government agencies in the extraordinary event that they believe those results warrant classification.*

Annex I: Members of the Commission on Scientific Communication and National Security

Co-Chairs

Harold Brown
Counselor & Trustee, CSIS;
Former Secretary of Defense

David Baltimore
President, Caltech;
Nobel Laureate for Physiology or Medicine

Members

William F. Ballhaus, Jr.
President and CEO, The Aerospace Corporation;
Former Director, NASA Ames Research Center

Paul Berg
Robert W. and Vivian K. Cahill Professor in Cancer Research, Stanford University;
Nobel Laureate for Chemistry

Alfred R. Berkeley III
Chairman of the Board of the Community of Science, Inc.
Former President and Vice Chairman, The NASDAQ Stock Market, Inc.

D. Allan Bromley (deceased February 2005)
Sterling Professor of the Sciences, Yale University;
Former Assistant to the President for Science and Technology Policy

Jared L. Cohon
President, Carnegie Mellon University

France Cordova
Chancellor, University of California, Riverside;
Former Chief Scientist, NASA

Charles B. Curtis
President and COO, Nuclear Threat Initiative;
Former Deputy Secretary, Department of Energy

James J. Duderstadt
President Emeritus and Professor of Science and Engineering, University of Michigan

Gerald R. Fink
Professor of Genetics, MIT;
Founding member and Former Director, Whitehead Institute for Biomedical Research

John Gage
Chief Researcher and Director of the Science Office, Sun Microsystems

Robert Gates
President, Texas A & M University;
Former Director of Central Intelligence

M.R.C. Greenwood
Provost and Senior Vice President - Academic Affairs, University of California;
Former Associate Director, White House Office of Science and Technology Policy (OSTP)

Margaret A. Hamburg
Senior Scientist and Former Vice President, Biological Programs, Nuclear Threat Initiative;
Former Assistant Secretary, Planning and Evaluation, Department of Health and Human Services

John P. Holdren
Heinz Professor of Environmental Policy, Kennedy School, Harvard University;
Former Member President's Committee of Advisors on Science and Technology (PCAST)

B.R. Inman
Lyndon B. Johnson Centennial Chair in National Policy, University of Texas at Austin;
Former Director, NSA; Former Deputy Director, CIA

Adel A. F. Mahmoud
President, Merck Vaccine Division

Richard A. Meserve
President, Carnegie Institution of Washington;
Former Chairman, Nuclear Regulatory Commission

Judith Miller
Partner Williams and Connelly;
Former General Counsel, Department of Defense

John S. Parker
Senior Vice President, SAIC;
Former Commanding General, United States Army Medical Research and Materiel Command

Elizabeth Rindskopf Parker
Dean, University of the Pacific – McGeorge School of Law;
Former General Counsel, NSA; Principal Deputy Legal Adviser, Department Of State; General Counsel, CIA

Phillip A. Sharp
Institute Professor, MIT; Director, McGovern Institute for Brain Research;
Nobel Laureate in Physiology or Medicine

Deanne Siemer
Managing Director, Wilsie Co. LLC
Former General Counsel, Department of Defense; Former special counsel to the President

George Terwilliger III
Attorney, White & Case, LLP;
Former Deputy Attorney General of the United States

Charles Vest
President Emeritus and Professor of Mechanical Engineering, Massachusetts Institute of Technology;
Member, President's Committee of Advisors on Science and Technology (PCAST)

Mitchel B. Wallerstein
Dean, Maxwell School of Citizenship and Public Affairs, Syracuse University;
Former Deputy Assistant Secretary of Defense for Counterproliferation Policy

Philip Zimmermann
Founder, Phil Zimmerman & Associates

Annex II: About the Commission on Scientific Communication and National Security

In partnership with CSIS, the National Academies in 2003 established the *Roundtable on Scientific Communication and National Security,* a deliberative body that represented a broad cross-section of the national security and scientific communities. The Roundtable provided a structured opportunity for the identification and discussion of the challenges posed by the potential conflicts between openness in science and requirements needed for enhanced national security. The roundtable format—a neutral discussion forum—enabled members of diverse and sometimes opposing institutions to engage in a continuing dialogue, and it provided them with the opportunity to build ongoing relationships that could, over time, facilitate collaboration. Consonant with policy and practices of the National Academies, the Roundtable did not make policy recommendations.

At the same time, the *Commission on Scientific Communication and National Security* (CSCANS) was created at CSIS with the same membership. Acting independently of the Roundtable, the Commission had the objective of generating actionable recommendations for public policy. This paper is a product of the CSIS Commission.

Goals

The CSIS-National Academies collaboration convened four times over a two-year period to discuss and study these issues as well as other urgent and ongoing issues associated with the central relationship between advancements in science and the preservation of security. The specific aims of the collaboration were:

- To foster dialogue between the science and technology and security communities as part of the process of formulating national policies regarding scientific collaboration and communication;
- To establish a focal point for unbiased and deliberative consideration of solutions to the dilemmas posed by balancing the need for open scientific communication with the need for protecting national and homeland security; and
- To propose policy-relevant research and analysis in this area.

Meeting these challenges is not a responsibility of the scientific community or the national security community alone; it requires an integrated effort. Science and security efforts must inform and support each other in order to successfully improve both the security and welfare of the United States.

Acknowledgments

The Commission would like to thank the Richard Lounsbery Foundation for providing support for this project, with special thanks to Maxmillian Angerholzer III for his guidance and assistance throughout the project. It would also like to thank CSIS Senior Associate Terence Murphy for his advice and review, as well as Alice Gast, Tobin Smith, and Patricia Wrightson, who also reviewed drafts of this document. Any remaining errors, of course, are solely the Commission's responsibility.

Annex III: CSIS Commission Staff

David Heyman
Senior Fellow and Director, Homeland Security Program

Gerald Epstein
Senior Fellow for Science and Security
Project Director, Commission for Scientific Communication and National Security
Homeland Security Program

Kate Phillips
Research Associate
Homeland Security Program

Lillian McTernan
Program Coordinator
Homeland Security Program

Daniel Rankin
Special Assistant
Office of Dr. Harold Brown