Order Code RL31845

# CRS Report for Congress

## "Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy

**Updated February 20, 2004**

Genevieve J. Knezo
Specialist in Science and Technology Policy
Resources, Science, and Industry Division




**Prepared for Members and Committees of Congress**



# "Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy


## Summary

The U.S. Government has always protected scientific and technical information that might compromise national security. Since the 2001 terrorist attacks, controls have been widened on access to information and scientific components that could threaten national security. The policy challenge is to balance science and security without compromising national security, scientific progress, and constitutional and statutory protections. This report summarizes (1) provisions of the Patent Law; Atomic Energy Act; International Traffic in Arms Control regulations; the USA PATRIOT Act, P.L. 107-56; the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, P.L. 107-188; and the Homeland Security Act, P.L. 107-296, that permit governmental restrictions on either privately generated or federally owned scientific and technical information that could harm national security; (2) the evolution of federal concepts of "sensitive but unclassified" (SBU) information; (3) controversies about pending Department of Homeland Security guidance on federal SBU and "Sensitive Homeland Security Information" (SHSI); and (4) policy options.

Even before the terrorist attacks of 2001, federal agencies used the label SBU to safeguard from public disclosure information that does not meet standards for classification in Executive Order 12958 or National Security Decision Directive 189. New Executive Order 13292 might widen the scope of scientific and technological information to be classified to deter terrorism. SBU has not been defined in statutory law. When using the term, some agencies refer to definitions for controlled information, such as "sensitive," in the Computer Security Act, and to information exempt from disclosure in the Freedom of Information Act (FOIA) and the Privacy Act. The identification of information to be released pursuant to these laws may be discretionary, subject to agency interpretation and risk analysis. The White House and the Department of Justice recently widened the applicability of SBU.

Critics say the lack of a clear SBU definition complicates designing policies to safeguard such information and that, if information needs to be safeguarded, it should be classified. Others say that wider controls will deny access to information needed for oversight and scientific communication. P.L. 107-296 required the President to issue guidance on safeguarding SBU homeland security information, a function assigned to the Department of Homeland Security Secretary in Executive Order 13311; action is pending. Issues of possible interest to Congress include designing uniform concepts and procedures to share and safeguard SBU information; standardizing penalties for unauthorized disclosure; designing an appeals process; assessing the pros and cons of wider SBU controls; and evaluating the implications of giving some research agency heads original classification authority. On February 20, 2004, DHS published a rule to protect voluntarily submitted critical infrastructure information. Some professional groups are starting to limit publication of some "sensitive" privately controlled scientific and technical information. Their actions may be guided by federal policy. This report will be updated as events warrant.

## Contents


Introduction . . . . . 1

Federal Controls on Privately Generated Scientific and Technical Information . . 1
Patent Law Secrecy . . . . . 1
The Atomic Energy Act and "Restricted Data" . . . . . 2

Export Control Regulations for Scientific and Technical Information . . . . . 3

Summary of Policies Regarding Classification of Scientific and Technical Research Results and Information . . . . . 6
Executive Order 12958, on "Classified National Security Information," as Amended by Executive Order 13292 . . . . . 6
National Security Decision Directive 189 (NSDD 189) . . . . . 7
Pre-Publication Review . . . . . 7

Controls on Information in the *USA PATRIOT Act* and in the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* . . . . . 9

"Sensitive But Unclassified" Information Restrictions . . . . . 10
Summary of the Evolution of Policies Relating to "Sensitive But Unclassified" Information . . . . . 11
Telecommunications Protection Policy *(PD/NSC-24)* . . . . . 11
National Security Decision Directive 145 *(NSDD-145)* . . . . . 11
The Computer Security Act of 1987 (P.L. 100-235) . . . . . 13
Computer Security in Relation to the Freedom of Information Act . . 14
Federal Agencies' Various Definitions of "Sensitive But Unclassified" . . 15
Introduction . . . . . 16
SBU in the State Department and U.S. Agency for International Development . . . . . 16
Defense Agencies' Use of SBU . . . . . 18
Department of Energy . . . . . 20
Other Agencies' Definitions of SBU, Including the General Services Administration, the Federal Aviation Administration, and the National Aeronautics and Space Administration . . . . . 20
Equivalence Between "Sensitive" and "Sensitive But Unclassified" Information . . . . . 21
White House Policy for "Sensitive but Unclassified" Information Related to Homeland Security, March 2002 . . . . . 23
Agencies Instructed to Use FOIA Exemptions to Control Disclosure of Information . . . . . 23

Policies for Control of Unclassified Information in P.L. 107-296 . . . . . 27
Introduction . . . . . 27
Protection of Critical Infrastructure Information . . . . . 27
"Sensitive But Unclassified" Homeland Security Information . . . . . 28
Federal Agency Implementation Actions . . . . . 29

Concerns About Sensitive Information in Non-governmental Research and Scientific Publications . . . . . 33
National Academies' Policy . . . . . 33
Other Groups . . . . . 34
Professional Groups Views That Scientists Should Voluntarily "Self-Regulate" Research and Publications . . . . . 36
Policy Options . . . . . 37

Policy Issues About "Sensitive But Unclassified" Information . . . . . 38
Introduction . . . . . 38
Historical Controversy About "Sensitive But Unclassified" . . . . . 38
Critiques of the White House (Card) Memorandum . . . . . 41

Policy Options for "Sensitive But Unclassified" Information . . . . . 42
Considerations Related to a Uniform Definition of SBU . . . . . 42
Factors Agencies Might Use in Developing Nondisclosure Policy for SBU Information . . . . . 46
The Potential to Classify More Research Information . . . . . 48
Appeals Process for SBU Information . . . . . 50
Determination of "Tiered" Access to SBU Information . . . . . 50

APPENDICES . . . . . 52
Appendix 2. Foreign Affairs Manual on SBU Information . . . . . 54
Appendix 3. Excerpts From ISOO/OIP Guidance, March 18, 2002 . . . . . 55

# Sensitive But Unclassified Information and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy

## Introduction

This report (1) summarizes provisions of several laws and regulations, including the Patent Law, the Atomic Energy Act, International Traffic in Arms Control regulations, the USA PATRIOT Act (P.L. 107-56), the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188), and the Homeland Security Act (P.L. 107-296), that permit the federal government to restrict disclosure of scientific and technical information that could harm national security; (2) describes the development of federal controls on "sensitive but unclassified" (SBU) scientific and technical information; (3) summarizes current controversies about White House policy on "Sensitive But Unclassified Information," and "Sensitive Homeland Security Information" (SHSI) issued in March 2002; and (4) identifies controversial issues which might affect the development of Office of Management and Budget (OMB) and agency guidelines for sensitive unclassified information, which are expected to be released during 2003.

## Federal Controls on Privately Generated Scientific and Technical Information

Several laws permit the federal government to classify privately-generated scientific and technical information that could harm national security, even when it is not held by federal agencies. These laws deal with patent law secrecy and atomic energy restricted data.

### Patent Law Secrecy

Pursuant to 35 U.S.C. 181-188, the U.S. Patent Commissioner has the right to issue patent secrecy orders to prevent disclosure of information about an invention if disclosure by granting of a patent would be detrimental to the national security. This provision is applicable to a patent for which the "government has a property interest" and those privately developed inventions which the government does not own. Thus, if a federal government agency has a "property interest" in the invention, the agency head will notify the Patent Commissioner, who is to withhold the publication of the application or the granting of a patent. If the government does not have a property interest in the patent and the Commissioner decides that the granting of a patent or publication of an application would be detrimental to the national

security, the Patent Commissioner is required to provide the patent application in question for inspection to the Atomic Energy Commission [now the Secretary of Energy], the Secretary of Defense, or the heads of other relevant agencies. If the agency head determines that publication or disclosure by the grant of patent is detrimental to the national security, the Patent Commissioner shall order that the invention be kept secret, and "shall withhold the grant of a patent ... for such period as the national interest requires...." The owner of the application may appeal the decision to the Secretary of Commerce. The invention may be kept secret for one year, but the Commerce Secretary may renew the secrecy order for additional periods as instructed by the agency head who initially determined the need for secrecy.[1]

If a secrecy order is issued during time of war, it shall remain in effect for the duration of hostilities and for one year following cessation of hostilities. If a secrecy order is issued during a national emergency, it shall remain in effect for the duration of the emergency and six months thereafter. The order may be rescinded by the Patent Commissioner upon written notification of the agency head who requested the order.

In addition, to prevent circumventing the law, a license must be obtained from the Patent Commissioner before a U.S. inventor files for a foreign patent application or registers a design or model with a foreign patent office. Penalties for violation of the law include a fine of not more than $10,000 or imprisonment for not more than two years, or both. During FY2002, 4,792 secrecy orders were in effect on patents applications; most of these were recommended by and issued to federal agencies for their own government-owned technical information; 37 were issued to individual private inventors.[2]

## The Atomic Energy Act and "Restricted Data"

Because of potential national security implications, nongovernmental scientists who conducted atomic energy research and development at the beginning of World War II took actions to keep such research secret, except for those with a need to know it. Strict governmental security during the war kept this knowledge limited, and after the war's end, the U.S. Congress passed the *Atomic Energy Act of 1946*,[3] which created the Atomic Energy Commission and established policies for securing atomic energy-related information. Atomic energy laws, as administered first by the Atomic Energy Commission and now the Department of Energy, allow the federal government to limit access to all atomic energy-related information, which is automatically "born classified" and is categorized upon creation as "restricted data," (RD), even if it is developed by private researchers outside of government. At first, access to this information was allowed only for defense purposes. Subsequent

---

[1] Source: Title 35, U.S.C. Secs. 181-188 (2000 ed.)

[2] Steven Aftergood, "New Invention Secrecy Orders Reported," *Secrecy News*, Jan. 6, 2003 referencing "Invention Secrecy Activity(as reported by the Patent & Trademark Office)," available at the Federation of American Scientists website at [http://www.fas.org/sgp/othergov/invention/stats.html].

[3] 60 Stat. 755.

modifications in law, principally the *Atomic Energy Act of 1954*, permitted certain non-governmental persons, such as industrialists and foreign governments, to obtain permits to access such "restricted data," for the purposes of peaceful commercial development of atomic energy or international cooperative programs if they could obtain the necessary security clearances.

"Restricted data," or RD, is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted data category pursuant to section 142 [42 USC 2162]."[4] Current penalties for violating the law include imprisonment for "any term of years," a fine of $100,000, or both.[5] The development and history of these controls were explained in a document prepared in 1989 by Arvin S. Quist, a classification officer at the Oak Ridge Gaseous Diffusion Plant, Oak Ridge National Laboratory, which is operated on contract for the Department of Energy. Excerpts from this document are included in **Appendix 1.**

## Export Control Regulations for Scientific and Technical Information

Both the Export Administration Act (50 U.S.C. App. 2401-2420)[6] and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals, both in the United States and abroad, of scientific and technical data related to items requiring export licenses according to the Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). Both laws regulate export of technical data.[7] ITAR control the release of defense articles specified on the U.S. Munitions List (22 CFR 121) and technical data

---

[4] Source: Atomic Energy General Provisions, 42 USC 2014 (2002), Definitions.

[5] 42 USC 2274 to 42 USC 2277, (2002).

[6] The Export Control Act has expired and the export control regulations are now operating under provisions of the International Emergency Economic Powers Act (IEEPA)pursuant to Executive Order 13222, issued August 17, 2001. For additional information on the reauthorization of the Export Administration Act of 1979, see CRS Report RL30169, *Export Administration Act of 1979 Reauthorization*, coordinated by Ian F. Fergusson.

[7] EAR define technical data as: "Information of any kind that can be used, or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a tangible form, such as a model, prototype, blueprints, or an operating model; or they may take an intangible form such as technical service" (15 CFR 772.1). The Department of Commerce implements the EAR regulations. ITAR define technical data as: "Information which is directly related to the design, engineering, development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, modification or reconstruction of defense articles. This includes, for example, information in the form of blueprints, drawings, photographs, plans, instructions, computer software and documentation. This also includes information which advances the state of the art of articles on the U.S. Munitions List. This does not include information concerning general scientific, mathematical, or engineering principles" (22 CFR 120.10). The Department of State implements the ITAR regulations.

directly related to them. EAR, among other things, control the export of dual-use items (items that have both civilian and military uses) on the [Department of] Commerce Control List (15 CFR Part 774) and technical data related to them. Licenses are needed to export controlled items. The implementing regulations are administered by the Department of Commerce, which licenses items subject to EAR, and by the Department of State, which licenses items subject to ITAR and the Munitions List of items.[8] They apply to "exporters" of both private and federally funded scientific and technical information. Fundamental research is excluded from ITAR and EAR.

ITAR generally treats the disclosure or transfer of technical data to a foreign national, whether in the United States or abroad as an export.[9] Some academic researchers believe they need to be registered with the State Department to hold conversations or meetings with foreigners in the United States about scientific developments.[10] According to ITAR regulations, publicly available scientific and technical information and academic exchanges and information presented at scientific meetings are not treated as controlled technical data.[11] Nevertheless, there has been considerable ambiguity and confusion regarding these provisions at some academic institutions because of uncertainties about which research projects might not be excluded because they use space or defense articles, technologies, and defense services on the Munitions List which is used to identify technologies requiring export licensing.[12] The Export Administration regulations also categorize as "deemed"

---

[8] See, for instance Office of Technology Assessment (OTA), *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* OTA-CIT-310, 1987, p. 142 and the "Corson" report, *Scientific Communication and National Security,* Committee on Science, Engineering, and Public Policy, National Academy Press, 1982.

[9] See 22 CFR 120.17 (4).

[10] This registration requirement applies only under the ITAR; however see the exception in 22 CFR 122.1 (b) (4), cited in footnote 11 below.

[11] 22 CFR 120.10(a)(5), 120.11. See also: International Traffic in Arms Regulations: Exemptions for U.S. Institutions of Higher Learning, 22 CFR Parts 123 and 125, *Federal Register,* Mar. 29, 2002, v. 67, no. 61, pp. 15099-15011. "Most notably, 22 CFR 122.1(b)(4) specifically exempts from the registration requirements of the ITAR 'persons who engage only in the fabrication of articles for experimental or scientific purpose, including research and development.' Further, specifically exempted from the definition of technical data is 'information concerning general scientific, mathematical or engineering principles commonly taught in schools, colleges, and universities,' 22 CFR 120.10(a)(5), and information that is in the 'public domain' if published and generally available and accessible to the public through, for example, sales at newsstands and bookstores, subscriptions, second class mail, and libraries open to the public, 22 CFR 120.11. Information is also in the public domain if it is made generally available to the public 'through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public in the United States' or 'through fundamental research in science and engineering at accredited institutions of higher learning in the U.S., where the resulting information is ordinarily published and shared broadly in the scientific community.' 22 CFR 120.11(6), (8)."

[12] Eugene B. Skolnikoff, "Research Universities and National Security: Can Traditional

(continued...)

exports communications to foreign nationals about technologies characterized as "sensitive" or countries identified as "sensitive" under EAR rules.[13] This is declaimed by some as a hindrance to international science and supported by others who view it as a needed national security protection.[14]

Since 1999, export of information about satellites and spacecraft instruments, including technical discussions about them, has been under the jurisdiction of the State Department and ITAR. Some academic researchers have complained that these rules curtailed their presentations at meetings, their on-campus research, and international collaborations because "research activity that once was subject to the fundamental research exclusion under National Security Directive 189, [See the next section for details] was, for the first time, formally regulated ...."[15] Reportedly, some foreign researchers at U.S. universities had not been able to access this information and U.S. researchers believed they needed a license to discuss defense-related basic research information with foreign colleagues. Universities sought clarifying rules.

Under a new rule issued in March 2002, the State Department clarified language exempting U.S. universities from obtaining ITAR licenses for export of certain[16] space-based fundamental research information or articles in the public domain to certain universities and research centers in countries that are members of the North Atlantic Treaty Organization (NATO), the European Union, or the European Space Agency, or to major non-NATO allies, such as Japan and Israel. Also to be permitted are exports of certain services and unclassified technical data for assembly of products into scientific, research, or experimental satellites. The exemption does not permit export of technical data for the integration of a satellite or spacecraft to a launch vehicle or Missile Technology Control Regime controlled defense services or technical data. A license will be needed for export of exempted information (including discussions) and hardware to researchers from all other countries. In addition, collaborators in approved countries would have to guarantee that researchers from non-approved countries were not receiving restricted information.[17]

---

[12] (...continued)
Values Survive?," Branscomb Lecture, Kennedy School of Government, Harvard University, Dec. 17, 2001, passim.

[13] 15 CFR 734.2(b).

[14] John J. Hamre, "Science and Security at Risk," *Issues in Science and Technology Online,* Summer 2002. According to Section 734.2 of the Export Administration Regulations, any release to a foreign national of technology or software subject to the regulations is deemed to be an export to the home country of the foreign national. These exports are commonly referred to as "deemed exports," and may involve the transfer of sensitive technology to foreign visitors or workers at U.S. research laboratories and private companies. Available at [http://w3.access.gpo.gov/bis/ear_data.html.]

[15] Association of American Universities, "ITAR and Universities: Universities Are Educational Institutions, Not Munitions Manufacturers," 2002 [www.aau.edu].

[16] Covered under category XV(a) or (e) of the U.S. Munitions List. These articles deal with spacecraft and associated data. (See 22 CFR Parts 123 and 125.)

[17] "International Traffic in Arms Regulations; Exemptions for U.S. Institutions of Higher
(continued...)

Some university researchers maintain that these rules do not go far enough in clarifying the situation and that academic researchers will find it difficult to design and implement campus controls and to bloc access to such information by students and scientists from disallowed countries.[18]

## Summary of Policies Regarding Classification of Scientific and Technical Research Results and Information

Several laws and directives govern classification of federally owned or federally funded scientific and technical research results or information. These are Executive Order (E.O.) 12958, National Security Decision Directive (NSDD) 189, and rules related to pre-publication review.

### Executive Order 12958, on "Classified National Security Information," as Amended by Executive Order 13292

Federal policy allows classification of federal information at three levels, "top secret," "secret," and "confidential." Until March 25, 2003, the most recent version of this policy was in Executive Order 12958, released on April 17, 1995.[19] It permitted classification of "scientific, technological, or economic matters relating to the national security" (Sec. 1.5). But Section 1.8 (b) prohibited classification of "basic scientific research information not related to the national security." On March 25, 2003, the President issued a new Executive Order 13292 on classification, which amended Executive Order 12958. It changed section 1.5 by adding a new clause, permitting classification of "scientific, technological, or economic matters relating to the national security, *which includes defense against transnational terrorism*"

---

[17] (...continued)
Education," Re: Department of State 22 CFR Parts 123 and 125 [Public Notice 3954], *Federal Register*, Mar. 29, 2002, pp. 15099-15101.

[18] Lawler, Andrew, "U.S. Export Controls: Rules Eased on Satellite Projects," *Science,* Apr. 12, 2002, pp. 237-238 and Gary G. Yerkey, "Export Controls: U.S. to Lower Restrictions on Trade in Products for Space-Based Research," *Daily Report for Executives,* Apr. 1. 2002, p. A-1.

[19] "Executive Order 12958, Classified National Security Information," Apr. 17, 1995. "Sec. 1.3. Classification Levels. ... (1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe. (2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe. (3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe. (b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information" (*Federal Register*, 60 FR 19825).

(Sec. 1.4 (e) of Executive Order 13292).[20] The amendment also added a new category of information which may be classified, that is information that concerns "weapons of mass destruction" (Sec. 1.4 (h)). The exemption for basic scientific research not clearly related to national security remains (renumbered section 1.7).

## National Security Decision Directive 189 (NSDD 189)

The policy embodied in Executive Order 12958 reflected prior policy expressed in *National Security Decision Directive 189, NSDD 189,* issued on September 21, 1985,[21] during the Reagan Administration. It says if federally funded basic scientific and technical information produced at colleges, universities and laboratories is to be controlled for national security reasons, it should be classified. But fundamental research findings generally are not to be restricted. Specifically, NSDD 189 states:

> ... to the maximum extent possible, the products of fundamental research[22] remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during Federally funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories is classification.

NSDD 189 made agencies sponsoring research responsible for determining, before the award of a research contract or grant, whether classification is appropriate and for periodically reviewing grants and contracts for potential classification.[23] It also said that "No restriction may be placed on the conduct or reporting of Federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes." NSDD 189 is still in effect, as stated in a letter issued by National Security Advisor Condoleeza Rice on November 1, 2001.[24]

## Pre-Publication Review

The federal government exercises "pre-publication review" of some privately published scientific and technical information by current and former employees and contractors who worked for federal agencies and who had access to classified

---

[20] (Emphasis added.) The White House, "Executive Order 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," March 25, 2003.

[21] See [http://www.aau.edu/research/ITAR-NSDD189.html].

[22] NSDD 189 defines "Fundamental research" as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

[23] See OTA, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* OTA-CIT-310, 1987, p. 143.

[24] See the letter at [http://www.fas.org/sgp/bush/cr110101.html].

information. For instance, the US Department of Agriculture issued the following guidance to employees regarding pre-publication review:

> In order to protect against the unauthorized disclosure of classified information, you are required to submit for security review any material intended for public release that might be based in any way on information you learned through your access to classified information. This requirement covers all written materials, including technical papers, books, articles, and manuscripts. It also includes lectures, speeches, films, videotapes. It includes works of fiction as well as non-fiction.[25]

Pre-publication review controls for research and development information may be written into federal government contracts. Typically the Defense Department (DoD) includes "pre-publication review" clauses in government contracts for extramural research that allow DoD to review research generated extramurally with federal support before it is published.[26] These controls are used if classified information was used in research or when the government seeks to prohibit release of information deemed sensitive because of the way it is aggregated.

An agreement was initiated in 1980 with the American Council on Education for all academic cryptography research to be submitted on a voluntary basis for pre-publication review to the federal government's National Security Agency.[27] Related to this, the U.S. Government may enter into contracts to purchase exclusive rights to commercial satellite imagery and has the ability to stop the collection and dissemination of commercial satellite imagery for national security reasons.[28]

In February 2002, DoD released a draft report, *Mandatory Procedures for Research and Technology Protection Within the DOD,* which would have required researchers to obtain DoD approval to discuss or publish findings of all military-sponsored unclassified research, a departure from existing policy guidelines. After

---

[25] Source: [http://www.usda.gov/da/ocpm/SecurityGuideEmployees/PrePubl.htm].

[26] See "Pre-publication Review of Web Site Content," at [http://www.iwar.org.uk/ecoespionage/resources/security-guide/S2unclas/Website.htm# Pre-Publication], citing "Web Site Administration Policies and Procedures," Nov. 25, 1998, Office of the Assistant Secrecy of Defense (C3I).

[27] Appendix E, in Computer Science and Telecommunications Board, *Cryptography's Role in Securing the Information Society,* National Academy of Sciences, 1996. The latest available commentary on this agreement dated 1996, indicates little or no negative impact on publication of cryptography research. For additional information, see: Chap. 5, in *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy,* Report of a Special Panel of the Association for Computing Machinery, Inc., U.S. Public Policy Committee (USACM) June 1994. by Susan Landau, et. al.

[28] James Randerson, *New Scientist Online News,* Oct. 17, 2001. See also Jessica Altschul, "Commercial Spy Satellites Pose a Challenge to Pentagon Planners," *JINSA Jewish Institute for National Security Affairs*, Feb. 28, 2002. U.S. Government controls appear to be authorized by Presidential Decision Directive 23 (PDD-23), Foreign Access To Remote Sensing Space Capabilities, Mar. 10, 1994. See also CRS Report RL31218 *Commercial Remote Sensing by Satellite: Status and Issues.*

academic objections, the draft was withdrawn; a revised and clearer set of new regulations is planned.[29]

## Controls on Information in the *USA PATRIOT Act* and in the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002*

Before the 2001 terrorist attacks, U.S. laboratories that transported "select agents," that is, about 40 dangerous biological agents and toxins, had to register with the federal government (42 CFR 72.6). Pursuant to the *USA PATRIOT Act,* P.L. 107-56 and the *Public Health Security and Bioterrorism Preparedness and Response Act of 2002,* P.L. 107-188, and the *Agricultural Bioterrorism Protection Act of 2002,* (which is part of P.L. 107-56), limits were placed on public access was extended to an additional 60 select agents, defined as "certain biological agents and toxins,"[30] whose misuse could pose security risks. Registration requirements were extended to include registration of persons who used these agents. To prohibit potential terrorists from access to these agents, controls were placed on access by selected persons, including those who could be potential terrorists, including criminals, illegal aliens, persons with mental defects, and or drug abusers; aliens not admitted for permanent residence from certain countries "which the Secretary of State has made a determination (that remains in effect) that such country has repeatedly provided support for acts of international terrorism,"[31] or persons who have been dishonorably discharged from the Armed Services. These controls will be administered by the Justice Department.[32]

Pursuant to these laws, the Departments of Health and Human Services and of Agriculture, identified the new list of "select agents," which was released in the *Federal Register* on December 13, 2002.[33] Under the interim final rule, which was amended on November 3, 2003,[34] the laboratories that use such agents will need to

---

[29] Ron Southwick, "Pentagon Backs Away From Strict Controls on Basic Research," *Chronicle of Higher Education,* May 31, 2002; interview with staff of International Security Programs, Office of the Deputy Under Secretary of Defense (Policy Support), April 2003.

[30] "Possession, Use, and Transfer of Select Agents and Toxins; Interim Final Rule," *Federal Register,* Dec. 13, 2002 (Vol. 67, No. 240), pp. 76885-76905.

[31] "Possession, Use, and Transfer of Select Agents and Toxins; Interim Final Rule," Dec. 13, 2002, op. cit.

[32] See CRS Report RL31263, *Public Health Security and Bioterrorism Preparedness and Response Act (P.L. 107-188): Provisions and Changes to Preexisting Law.*

[33] The list of agents published in the *Federal Register*, "Possession, Use, and Transfer of Select Agents and Toxins; Interim Final Rule," Dec. 13, 2002, op. cit. is available at [http://www.fas.org/sgp/news/2002/12/ag121302.html] and [http://www.fas.org/sgp/news/2002/12/hhs121302.html]. The Center for Disease Control and Prevention's (CDC) fact sheet is at [http://www.cdc.gov/od/sap/docs/faq.pdf].

[34] "Possession, Use, and Transfer of Select Agents and Toxins; Interim Final Rule and (continued...)

register and control access to such agents; scientists will have to register, submit to background checks, and obtain prior approval to use, send, or receive select agents used in experiments. Some say this process, while denying access to possible terrorists, might prove costly and burdensome to some researchers (estimated in an article by Malakoff at $700,000 per laboratory)[35] and has the potential of limiting the conduct of some scientific research that would otherwise be performed by such persons, including some foreign researchers. In addition, privately funded scientists will be subject to the same requirements as government-funded researchers who need "prior approval from the DHHS ... for genetic engineering experiments that might make a select agent more toxic or more resistant to known drugs."[36] Civilian and criminal penalties for noncompliance apply to universities, private companies and government laboratories. Laboratories that handle select agents were to be in compliance with the new rules by fall 2003.

## "Sensitive But Unclassified" Information Restrictions

Over time some agencies have established procedures to identify and safeguard "sensitive but unclassified information" (SBU), also called "sensitive unclassified information." Generally, this unclassified information is withheld from the public for a variety of reasons, but needs to be accessible to federal agency personnel. As will be discussed next in this report, the term SBU has been defined in various presidential-level directives and agency guidances, but, some critics say, only indirectly in statute. Agencies have given the term various meanings in their implementing rules and regulations. Some agency guidance documents have started to use interchangeably the terms "for official use only," "limited use," "sensitive," "sensitive but unclassified," and related terms, and have defined SBU by referring to such statutes as *Privacy Act of 1974* (5 USC 552a),[37] the *Freedom of Information Act (FOIA) of 1966* (5 USC 552 ), the *Computer Security Act of 1987* (relevant portions codified at 15 USC 278 g-3), and other language. Agencies have discretion to define SBU in ways that serve their particular needs to safeguard information. There is no uniformity in implementing rules throughout the government on the use of SBU. Agencies also may assign various criminal and civilian penalties to improper release of "sensitive but unclassified" information.

---

[34] (...continued)
Request for Comments," *Federal Register,* Nov. 3, 2003 (Vol. 68, No. 212) pp. 62245-62247.

[35] David Malakoff, "New U.S. Rules Set the Stage for Tighter Security, Oversight," *Science,* Dec. 20, 2002, p. 2304.

[36] Malakoff, Dec. 20, 2002, op. cit.

[37] P.L. 93-579, which prohibits the release of individual personal information held by the federal government pertaining, but not limited to "education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."

## Summary of the Evolution of Policies Relating to "Sensitive But Unclassified" Information

Official definitions of SBU were issued as early as 1977 and over the years thereafter.

***Telecommunications Protection Policy (PD/NSC-24).*** In 1977, in one of the earliest references to SBU, a Presidential Directive on *Telecommunications Protection Policy (PD/NSC-24)* mandated protection of unclassified, but sensitive communications "that could be useful to an adversary." It did not define the term further.[38]

***National Security Decision Directive 145 (NSDD-145).*** In 1984, *National Security Decision Directive 145 (NSDD-145)* directed 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 threat of exploitation and the associated potential damage to the national security." NSDD-145 did not define the term, "sensitive, but unclassified," but explained that even unclassified information in the aggregate can "reveal highly classified and other sensitive information ..." harmful to the national security interest.[39]

The absence of a precise definition was widely criticized, especially by the General Accounting Office (GAO)[40] because of concern that the 1984 definition of

---

[38] Presidential Directive/National Security Council-24 (PD/NSC-24), signed by President Jimmy Carter in 1977, has been partially unclassified. "PD/NSC-24 directed Federal department heads to protect unclassified, but sensitive communications, and it assigned responsibility to DoD for the security of classified communications and for unclassified, but sensitive communications related to national security" (OTA, *Defending Secrets....*, p.137).

[39] *National Security Decision Directive (NSDD-145)*, on "National Policy on Telecommunications and Automated Information Systems Security," Sept. 17, 1984, essentially replaced PD/NSC-24. It was developed by DoD and it "authorized the Director of the National Security Agency to review and approve all security-related standards for information systems, including those set by the National Institute of Standards and Technology in the Department of Commerce. (U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions," Report to the Honorable Jack Brooks, Chairman, Committee on the Judiciary, House of Representatives,"* Nov. 1993, GAO/OSI-94-2, p. 15.) It also established policy and an interagency organizational structure to guide the conduct of national activities to safeguard systems that process, store, or communicate sensitive information. The interagency structure, headed by the presidential advisor for National Security Affairs, included not only defense and intelligence agencies, but some civilian agencies. Its responsibilities were to implement information classification policies and to develop computer security protections for information security.

[40] In congressional testimony in 1985, GAO complained that this directive could possibly give national security agencies control of the management systems of civilian agencies and private commercial interests "... because it established a new category of 'sensitive, unclassified government or government-derived information, the loss of which could adversely affect the national security interest....' without clearly defining the types of

(continued...)

SBU could include national security-related as well as possibly innocuous information needed to make policy. For instance, a GAO witness testified, "... unclassified sensitive civil agency information affecting national security interests could include hazardous materials information held by the Department of Transportation, flight safety information held by the Federal Aviation Administration, and monetary policy information held by the Federal Reserve." He recommended that the Administration "needs to clearly define the types of information that fall under the coverage of NSDD-145."[41]

*National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2* On October 29, 1986, President Reagan's National Security Advisor, John Poindexter,[42] issued a document, entitled *National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2*, that widened the rationale for safeguarding "sensitive, but unclassified" information for reasons of national security, as in NSDD-145, to include also "other government interests." Specifically, it said,

> Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

---

[40] (...continued)
information in this category."(GAO/OSI-94-2, p. 15.) Except for activities mandated by it and by Presidential Directive-24 (issued by President Carter in 1977) pertaining to telecommunications information protection activities, NSDD-145 was rescinded by National Security Directive 42 (National Policy for the Security of National Security Telecommunications and Information Systems), July 5, 1990. (Kenneth W. Dam and Herbert S. Lin, eds., *Cryptography's Role in Security the Information Society,* National Academy of Sciences, 1996. Full text of NSDD-145 is at ]www.fas.org/irp/offdocs/nsdd145.htm].

[41] "The Potential Impact of National Security Decision Directive (NSDD) 145 on Civil Agencies," Warren G. Reed, GAO, before the Subcommittee on Transportation, Aviation, and Materials, Committee on Science and Technology, June 17, 1985.

[42] Currently head of the Defense Advanced Research Projects Agency's Total Information Awareness research program. See: Shane Harris, "Senate Moves to Block Pentagons Anti-terror Data Mining Effort," *GovExec.com.* Jan. 24, 2003. On the TIA program, see CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws.*

This policy was to be applicable to all federal executive departments and agencies, including their contractors, which electronically transferred, stored, processed, or communicated sensitive, but unclassified information.[43]

During 1986-1987, criticisms about NTISSP No. 2 focused on both the scope of information to be restricted and the responsibility given to the intelligence community over civilian information activities. These led to the withdrawal of both NTISSP No. 2 in 1987 (attendant to passage of the Computer Security Act of 1987) and to official use of this definition of "sensitive, but unclassified."[44] (However, as will be noted below, some agencies, notably the Department of Energy, still use this broad conceptualization of SBU.)

**The Computer Security Act of 1987 (P.L. 100-235).** In the Computer Security Act of 1987 (P.L. 100-235, 101 Stat. 1724-1730), 40 USC 1441, Congress declared: "... improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use" (Section 2, Purpose). The law authorized creation of a computer standards program within the National Bureau of Standards, now called the National Institute of Standards and Technology (NIST)), actions to enhance Government-wide computer security, and training in security matters for persons who are involved in the management, operation, and use of Federal computer systems.

P.L. 100-235 also addressed some of the criticisms raised about NTISSP No. 2. It defined the term "sensitive" as

> any information, the loss, misuse, or unauthorized access to or modification of which *could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act)*, but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy" (Section 3). (Emphasis added.)

The last clause of this definition specifically limited the definition of "sensitive" to information that was not classified. Agencies were given discretion to identify information that was sensitive and risks accompanying release of it. The report accompanying the bill said that each individual federal agency should make a

---

[43] Appendix B. "National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, National Telecommunications and Information Systems Security Policy, "NTISSP No. 2, Oct. 29, 1986, Issued by John Poindexter," in OTA, *Defending Secrets....*, p. 166.)

[44] This occurred after congressional hearings in February and March 1987 following negotiations between executive branch officials and Members of Congress and committees having jurisdiction over H.R. 145, a bill which became the Computer Security Act of 1987, P.L. 100-235. Subsequently "the National Security Council initiated a review of NSDD-145 aimed at reducing or eliminating its operational role" and the civilian agency participation in the NTISSC was expanded (*Defending Secrets...*, pp. 144, 148).

determination of which unclassified information in its systems was sensitive in accord with the definition of sensitive in the law and the purposes of the law.[45] Federal agencies were given responsibility for developing plans "commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information being protected," and are responsible for protecting such "sensitive" information.[46]

In 1992 the National Institute of Standards and Technology (NIST) issued guidance about agency implementation of systems to protect sensitive information pursuant to P.L. 100-235. It reiterated that,

> Interpretation of the Computer Security Act's definition of sensitive is, ultimately, an agency responsibility. Typically, protecting sensitive information means providing for one or more of the following: *Confidentiality*: disclosure of the information must be restricted to designated parties; *Integrity*: The information must be protected from errors or unauthorized modification; *Availability*: The information must be available within some given time frame (i.e., protected against destruction)."[47]

The NIST document urged agency information owners to "use a risk-based approach to determine" harm of inadequate protection of information. In defining this discretionary process, it emphasized,

> Information 'owners,' not system operators, should determine what protection their information requires. The type and amount of protection needed depends on the nature of the information and the environment in which it is processed. The controls to be used will depend on the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in the system.[48]

Because P.L. 100-235 applied to "sensitive" information that is not classified, some say, in effect, it defined "sensitive but unclassified."

**Computer Security in Relation to the Freedom of Information Act.** The Freedom of Information Act of 1966 (FOIA) was enacted to ensure public access to certain types of information held by federal agencies. However, it permits agencies to exempt from public disclosure nine types of information:

(1) information classified in the interest of national defense or foreign policy,
(2) internal personnel rules and practices of an agency,
(3) information specifically exempted from disclosure by statute,

---

[45] Section 6 of P.L. 100-235 and Section on "Training," in U.S. Congress, House, Committee on Science and Technology, *Computer Security Act of 1987,* Report to Accompany H.R. 145, June 11, 1987.

[46] U.S. Congress, House, Committee on Science and Technology, *Computer Security Act of 1987,* Report to Accompany H.R. 145, June 11, 1987, pp. 30-31.

[47] CSL Bulletin: "Advising Users on Computer System Technology," Nov. 1992 [http://nsi.org/Library/Compsec/sensitiv.txt]. (Emphasis added.) This is published by NIST.

[48] CSL Bulletin: "Advising Users on Computer System Technology," Nov. 1992.

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential,
(5) inter-agency or intra-agency memoranda or letters reflecting predecisional attitudes,
(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,
(7) specified types of law enforcement records or information,
(8) financial institution regulation or supervision reports, and
(9) geological and geophysical information and data concerning wells.[49]

As noted above, the definition of "sensitive" in the Computer Security Act cited three reasons to categorize non-classified information as sensitive: adverse effects on the national interest, adverse effects on the conduct of federal programs, and privacy. It included explicit provisions saying it was not authority to withhold information sought pursuant to "section 552 of title 5, United States Code [the Freedom of Information Act]...."[50] This was reiterated in 1992 when the National Institute of Standards and Technology issued guidance about agency implementation of systems to protect sensitive information pursuant to P.L. 100-235.[51] Neither the Computer Security Act nor the accompanying report indicated that information exempt from FOIA was to be designated as "sensitive." Also, the report accompanying the legislation said specifically, "The designation of information as sensitive [or as subject to protection] under the Computer Security Act is not a determination that the information is not subject to public disclosure."[52]

However, major federal agencies started to apply the label SBU to information defined as "sensitive" in the Computer Security Act and to information exempt from disclosure under the Freedom of Information Act (especially as governed by provisions 2 and 4). In fact, some agencies have declared that these acts define SBU, a statement which is open to debate.

## Federal Agencies' Various Definitions of "Sensitive But Unclassified"

---

[49] Source: 5 USC 552.

[50] According to "Sec. 8. Rules of Construction of Act. Nothing in this Act, or in any amendment made by this Act, shall be construed — (1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or (2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is — (A) privately-owned information; (B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or (C) public domain information."

[51] The guidance said: "The Computer Security Act did not alter the Freedom of Information Act (FOIA); therefore, an agency's determination of sensitivity under this definition does not change the status of releaseability under the FOIA." (CSL Bulletin: "Advising Users on Computer system Technology," Nov. 1992 [http://nsi.org/Library/Compsec/sensitiv.txt].

[52] House Report 100-153, Part I, June 11, 1987.

**Introduction.** Even before the terrorist attacks of September 2001 and actions taken by the White House during 2001 and 2002 to safeguard "sensitive but unclassified" information, federal agencies had implemented a variety of procedures to safeguard information. While they have used classification categories to withhold information classified pursuant to Executive Order 12958, they also use a variety of administrative control markings and procedures to control access to unclassified information to which public access is restricted, such as privacy data, law enforcement information, health information, and information exempt from disclosure under the Freedom of Information Act (FOIA), and "sensitive" information. According to a report of the *Commission on Protecting and Reducing Government Secrecy, 1997*, "... at least 52 different protective markings [are] being used on unclassified information, approximately 40 of which are used by departments and agencies that also classify information. Included among these are widely-used markings such as 'Sensitive But Unclassified,' 'Limited Official Use,' 'Official Use Only,' and 'For Official Use Only.' "[53] Other notable categories are Drug Enforcement Administration (DEA) sensitive information, and DoD Unclassified Controlled Nuclear Information.[54]

There is no uniformity in Federal agency definitions, or rules to implement safeguards for "sensitive but unclassified" information. Over time the term "sensitive but unclassified" has come to be used to encompass information subject to control pursuant to the Computer Security Act, as well as information determined to be exempt from disclosure under the Freedom of Information Act, 5 USC 552. This is further complicated by the fact that, as noted above, agencies were given discretion under the Computer Security Act of 1987 to do risk analysis to identify information to be safeguarded as sensitive. In addition , as will be described below, since the terrorist attacks of 2001, the Bush Administration has given agencies discretion to make nondisclosure decisions under FOIA in relation to homeland security and the thwarting of terrorist attacks.

**SBU in the State Department and U.S. Agency for International Development.** In its *Foreign Affairs Manual,* issued on October 1, 1995, the Department of State said it would stop using the designation "limited official use," (LOU), which it had applied to information exempt from FOIA disclosure, and in its place would use the term "sensitive but unclassified" (SBU).[55] This appears to have been one of the earliest instances of an agency declaring that SBU applies to information exempt from disclosure under the Privacy Act as well as under the Freedom of Information Act:

> a. SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public

---

[53] *Report of the Commission on Protecting and Reducing Government Secrecy, 1997,* Senate Document 105-2, Pursuant to P.L. 236, 103rd Congress, 1997, Chap. II, Section on "Protecting Other Government Information," [http://www.fas.org/sgp/library/moynihan/chap2.html]. This is also called the Moynihan Commission Report on Government Secrecy.

[54] See [http://www.fas.org/irp/doddir/dod/5200-1r/appendix_c.htm].

[55] Foreign Affairs Manual: SBU Information, [http://foia.state.gov/docs/12fam/12m0540.pdf].

> disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. (12 FAM 540, Sensitive but Unclassified Information (SBU), (TL: DS-61; 10-01-1999) 12 FAM 541 SCOPE, (TL: DS-46; 05-26-1995).

The State Department declared that,

> b. SBU information includes, but is not limited to:
>
> (1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and (2) Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. (12 FAM 540, Sensitive but Unclassified Information (SBU), (TL: DS-61; 10-01-1999) 12 FAM 541 SCOPE, (TL: DS-46; 05-26-1995).

In an explanatory telegram sent to U.S. embassies, the department explained why it would use the SBU category instead of the LOU category and it declared that SBU covered information exempt from FOIA. It said, "Sensitive but unclassified is not a classification level for national security information, but is used when it's necessary to provide a degree of protection from unauthorized disclosure for unclassified information as set forth in 12 FAM 540."[56] It explained that it would use the category of SBU for two reasons: "... to keep classified material to a minimum and to be able to pass-on relevant, but sensitive information to individuals (including FSNS [Foreign Service National staff]) on a need to know bases (sic)."[57] Public access to "sensitive but unclassified" information would be limited to those with a need to know and would be subject to provisions which govern disclosure and exemptions in the Freedom of Information Act and Privacy Act; unauthorized disclosure would be subject to criminal penalties, including "criminal and/or civil penalties. Supervisors may take disciplinary action, as appropriate."[58]

---

[56] "Dept. of State Telegram, to All Diplomatic and Consular Posts US Office Pristina Special Embassy Program Executive Order 12958: N/a Tags: Acoa Subject: Guidance for Drafting SBU," Telegram Ref: 95 State 232445, (Source: [http://www.fas.org/sgp/news/2000/02/sbu.html]).

[57] "Dept. of State Telegram, to All Diplomatic and Consular Posts US Office Pristina Special Embassy Program Executive Order 12958: N/a Tags: Acoa Subject: Guidance for Drafting SBU," Telegram Ref: 95 State 232445, (Source: [http://www.fas.org/sgp/news/2000/02/sbu.html]). It described this designation as an "administrative control marking" to protect "documents that do not contain national security information but must be protected from disclosure. This control designation must appear at the top and bottom of any cover, title page, first page, and last page of the document." FAH-1-H-135, Administrative Control Marking," in U.S. Department of State, *Foreign Affairs Handbook,* Correspondence, p. 3 of 3.

[58] "12 FAM 545, Responsibilities," U.S. Department of State, *Foreign Affairs Handbook,* p. 2 of 2.

In 1995, the U.S. Agency for International Development equated "sensitive" with "sensitive but unclassified" and linked procedures needed to protect "sensitive but unclassified" to protections required by FOIA and the Computer Security Act.[59]

**Defense Agencies' Use of SBU.** DoD's guidance for "controlled unclassified information," issued in 1997, stated that "For Official Use Only (FOUO)" designations should be used for unclassified information that should be protected, that this includes "information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA)" and "sensitive but unclassified" information that the Department of State formerly designated as Limited Official Use (which meets the criteria for exemption from mandatory public disclosure under FOIA), and "there must be a legitimate Government purpose served by withholding it."[60] This same DoD directive limited dissemination of information labeled "for official use only" including "sensitive but unclassified" information to:

> ... within the DoD Components and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other

---

[59] The U.S. Agency for International Development issued a general notice on November 9, 1995, subsequently reprinted in 1997 as "USAID/General Notice M/IRM, 2/3/97," which said, "... AID ... has adopted the term "sensitive but unclassified (SBU)".... [T]he term "SBU" supersedes the terms "sensitive data" or "sensitive information."*[A]lways* considered SBU information is "procurement source evaluation and source selection, company proprietary, investigative, restricted scientific/technical information, and travel plans of USAID employees to or through a high or critical terrorist threat environment. The following categories of information are considered potential SBU information: legal, financial, budget projections, medical, contractual, procurement, intellectual property, agency-critical or foreign government. Each creator or handler of potential SBU information must make the sensitive/non-sensitive determination on a case-by-case basis." Disclosure of such information was authorized "on a clearly demonstrated need to know or need to use" basis. If the information were transmitted electronically, it would have to be encrypted and staff were warned that " ... unauthorized disclosure of SBU information may result in criminal and/or civil penalties." The document also listed the nine exemptions permitted by FOIA and emphasized that "... section (3) of the FOIA has been interpreted to include statutes such as the Computer Security Act of 1987...." Information owners who choose to exempt their information for very specific reasons from public disclosure under a FOIA request are required by the SBU policy to consider their exempted data SBU information and protect it accordingly." ([Http://csrc.nist.gov/fasp/FASPDocs/systemsec-plan/USAID SecurityPlanBSPT5.htm ].)

[60] "Appendix 3C, Controlled Unclassified Information," In DoD 5200.1-R, Information Security Program, Jan. 1997, issued by Assistant Secretary of Defense for Command, Control, Communications and Intelligence. It also said that if Department of State SBU information were included in a DoD document, it should be "marked as if the information were "For Official Use Only." Other kinds of unclassified but controlled information that are to be handled as FOUO information, according to DoD are Drug Enforcement Administrative Sensitive Information, DoD Unclassified Controlled Nuclear Information, and Sensitive Information, as defined by the Computer Security Act of 1987. (Secs. 2 and 6). See: Appendix C. "Controlled unclassified Information," Section 3, [http://www.fas.org/irp/doddir/dod/5200-1r/appendix_c.htm]. See also Guidance for Telework Involving Sensitive-Unclassified information, prepared by Naval Air Warfare Center Aircraft Division, [http://hro.navair.nay.mil/telework/sensunclass.htm].

> Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. (Special restrictions may apply to information covered by the Privacy Act.) Release of FOUO information to Members of Congress is covered by DoD Directive 5400.4, and to the General Accounting Office by DoD Directive 7650.1."[61]

According to the U.S. Army, citing DoD Regulation 5200.1 and Army Regulation 25-55, SBU information is information exempted from disclosure under FOIA. Also, Army Regulation 380-19, Section 1-5, "gives some examples of SBU as information that: (a) involves intelligence activities, (b) involves cryptological activities related to national security, (c) involves command and control of forces, (d) is contained in systems that are an integral part of weapon or a weapon system; (e) is contained in systems that are critical to the direct fulfillment of military or intelligence missions, (f) involves processing of research, development, and engineering data."[62]

The U.S. Army Materiel Command encrypts certain categories of SBU data, including "logistics, medical care, personnel management, Privacy Act data, contractual data, and "For Official Use Only Information."[63] Since there is no one source for a definition of SBU, according to this source, "Other factors such as risk management, consideration of the effects of unauthorized disclosure, and an examination of the timeliness of information, should be taken into account as well. Ultimately level of sensitivity of the information should be determined by owner/creator of the data."[64] A matrix presented that guides the definition of SBU follows. Note that certain research and development data are included:

SBU MATRIX[65]

> The matrix below provides a general guide on the data categories and description of the types of data that should be considered Sensitive But Unclassified. This matrix should not be considered authoritative or all-inclusive.

| Data Category | **Description** |
|---|---|
| FOIA Exempted | Any information that is exempted from mandatory disclosure under the Freedom of Information Act. |
| Intelligence Activities | Information that involves or is related in intelligence activities, including collection methods, personnel, and unclassified information. |

---

[61] 2-202 Access to FOUO Information, [http://www.fas.org/irp/doddir/dod/5200-1r/appendix_c.htm].

[62] Cited in Stuart D. Smith, "Sensitive But Unclassified Data; Identification and Protection Solutions,"Prepared for U.S. Army Material Command Information Assurance Program Manager, July 2002, pp. 4-5.

[63] Smith, op. cit., p. 5.

[64] Smith, op. cit., p. 6.

[65] Smith, op. cit., p. 13.

| Data Category | Description |
|---|---|
| Cryptologic Activities | Information that involves encryption/decryption of information; communications security equipment, keys, algorithms, processes; information involving the methods and internal workings of cryptologic equipment. |
| Command and Control | Information involving the command and control of forces, troop movements. |
| Weapon and Weapon Systems | Information that deals with the design, functionality, and capabilities of weapons and weapon systems both fielded and un-fielded. |
| RD&E | Research, development, and engineering data on un-fielded products, projects, systems, and programs that are in the development or acquisition phase. |
| Logistics | Information dealing with logistics, supplies, materials, parts and parts requisitions, including quantities and numbers. |
| Medical Care/HIPAA | Information dealing with personal medical care, patient treatment, prescriptions, physician notes, patient charts, x-rays, diagnosis, etc. |
| Personnel Management | Information dealing with personnel, including evaluations, individual salaries, assignments, and internal personnel management. |
| Privacy Act Data | Information covered by the Privacy Act of 1974 (5 U.S.C. § 552A) |
| Contractual Data | Information and records pertaining to contracts, bids, proposals, and other data involving government contracts. |
| Investigative Data | Information and data pertaining to official criminal and civil investigations such as investigator notes and attorney-client privileged information. |

**Department of Energy.** The Department of Energy (DOE) uses a definition of "sensitive but unclassified" which is identical to the 1986 Poindexter definition that Congress had the Administration withdraw. It is:

> *Sensitive Unclassified Information:* Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Governmental interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentially of personal or commercial proprietary information provided to the U.S. Government by its citizens.[66]

Guidance used by the DOE laboratories refers to this concept and cites, as authority, Executive Order 12958 and DOE regulations.[67]

**Other Agencies' Definitions of SBU, Including the General Services Administration, the Federal Aviation Administration, and the National Aeronautics and Space Administration.** Other agencies have issued directives to define and prescribe safeguards that should be taken and penalties used

---

[66] U.S. Department of Energy, *Safeguards and Security: Glossary* , Dec. 18, 1995, p. 132.

[67] Source: Executive Order 12958, "Classified National Security Information," Apr. 17, 1995 and DOE O 471.2A, Information Security Program, Mar. 27, 1997, at [http://www.oa.doe.gov/sase/directives/o4712a.pdf], and *Draft DOE Glossary*, [http://labs.ucop.edu/internet/security/brief00].

for releasing SBU information. For instance, in 2002 the General Services Administration (GSA) defined SBU to include information that could possibly benefit terrorists, such as equipment plans, building designs, operating plans, the locations of secure facilities or functions within GSA buildings, utility locations, and information about security systems or guards.[68] The Federal Aviation Administration (FAA) issued regulations to safeguard unclassified but "sensitive security information," which may be developed from security or research and development activities and whose release, the Administration determines, could be an invasion of personal privacy, reveal private or financial information, or could "be detrimental to the safety of passengers in transportation."[69]

The National Aeronautics and Space Administration (NASA) labels nonclassified sensitive information as "administratively controlled information (ACI)," and describes procedures for controlling it under the same heading that it uses to describe procedures to control classified national security information (CNSI):

> Such information and material, which may be exempt from disclosure by statute or is determined by a designated NASA official to be especially sensitive, shall be afforded physical protection sufficient to safeguard it from unauthorized disclosure. Within NASA, such information has previously been designated "For Official Use Only."[70]

The statutes cited as justification are the Export Administration Act of 1979, the Arms Export Control Act, and section 303 (b) of the Space Act. NASA also cited as justification the exemption criteria of the Freedom of Information Act, and information designated by NASA officials, such as predecisional and not-yet-released materials relating to national space policy, pending reorganization plans, or sensitive travel itineraries.

In some agencies, the official responsible for guiding and developing agency policy and procedure for classified information also has responsibility for control and decontrol of sensitive but unclassified information.[71]

## Equivalence Between "Sensitive" and "Sensitive But Unclassified" Information

By 1997, the Department of the Navy had issued guidance that said explicitly that the Computer Security Act of 1987 defined the requirements for "sensitive but

---

[68] General Services Administration, Public Buildings Services Order 3490.1, Mar. 8, 2002.

[69] Authorized by Title 49 U.S.C. 40119; regulations were included in Title 14 CFR Part 191.

[70] Section 4.4.7.2 of Chap. 4, "Information Security," in NASA Security Procedures and Guidelines With Change 1, Sept. 13, 2002.

[71] "Delegation of Authority for Physical Security Programs," Department of the Army, Directive 71-08, Apr. 26, 1999.

unclassified" information and further that "all business conducted within the federal government is sensitive but unclassified."[72]

In 1998, the equivalence between "sensitive" and "sensitive but unclassified" was codified by DoD in administrative law in 32 CFR 149.3, relating to technical surveillance countermeasures used by all federal agencies that process SBU. DoD defined "sensitive but unclassified" by using the definition of "sensitive" that appeared in the Computer Security Act of 1987.[73]

---

[72] According to the Navy, the nature of its mission, "accompanied by connectivity and data aggregation issues, has led to the determination that all unclassified information processed by DON information systems is sensitive" ("Fundamental Infosec Policy," Department of the Navy Information Systems Security (INGODSRV) Program, SECNAVINST 5239.3, July 14, 1995. The source is [http://www.fas.org/irp/doddir/navy/secnavinst/5239_3.htm]. Also available at [http://www.onr.navy.mil/sci_tech/industrial/nardic/pubs_list.asp?Letter=S].

The Navy's Contractor Performance Assessment Reporting System documentation, said that: "The Computer Security Act of 1987 defines the requirements for Sensitive But Unclassified data (SBU) and supports the premise that essentially all business conducted within the federal government is SBU. SBU is to be protected in federal computer systems (including contractors). ... SECNAVINST 5239.3 ... defines SBU...." According to this system, the Navy has defined nine categories of "sensitive but unclassified" information as follows:

- Proprietary Data: Trade secrets and commercial or financial information obtained from a person and privileged or confidential.
- For Official Use Only: Categories of information exempt from public release under the provisions of the Freedom of Information Act. Documents containing FOIA exempt information are identified by the caveat "For Official Use Only."
- Treaties & International Agreements: Information which must be protected in accordance with the stipulations of a particular treaty or international agreement such as the Chemical Weapons Compliance Treaty or North American Free Trade Agreement.
- Technical Military Data: Technical data with military or space application which may not be exported lawfully outside the U.S. without prior approval, authorization, or license under the Export Act of 1979 or the Arms Export Control Act.
- Export Control Data: Data which is subject to export controls (international traffic in arms regulation, export control act, U.S. munitions list).
- Competition Sensitive Data Data associated with ongoing procurement of government supplies, services or equipment to include contractor bids and proposals and associated government documents.
- Privacy Act: Information which must be protected from public release to protect the privacy of the individual (social security number, investigative data, payroll records, disciplinary records, etc.).
- Investigative and Inquiry Data: Information associated with or resulting from criminal, civil, security, inspector general, flight safety, or other investigations or inquiries which must be protected from public release.
- Naval Nuclear Propulsion Information: Information concerning the design and operation of Naval nuclear reactors and associated equipment which does not meet the criteria for classification under Executive Order 12958. ("Contractor Performance Assessment Reporting System, Frequently Asked Questions Page," [http://cpars.navy.mil/cparsfiles/sbu.asp].) CPARS is the Department of the Navy's Contractor Performance Assessment Reporting System, maintained by the Naval Sea Logistics Center, Portsmouth, New Hampshire.

[73] "National Policy on Technical Surveillance Countermeasures," issued by the Office of the (continued...)

In 2002, the Department of the Interior issued guidance that "... all unclassified DOI systems are considered SBU."[74]

## White House Policy for "Sensitive but Unclassified" Information Related to Homeland Security, March 2002

On March 19, 2002, the White House released a memo, signed by Chief of Staff Andrew Card, entitled "Action to Safeguard Information Regarding Weapons of Mass Destruction and other Sensitive Documents Related to Homeland Security." It called for agencies to reconsider current measures for safeguarding information regarding weapons of mass destruction and other sensitive documents related to homeland security and "information that could be misused to harm the security of our Nation and the safety of our people." Agencies were required to examine their policies and holdings in accord with an accompanying memos issued by the National Archives and Records Administration's (NARA) Information Security Oversight Office (ISOO) and the Department of Justice's Office of Information and Privacy (OIP) to determine if information should be classified, including previously unclassified or declassified information, or handled as sensitive but unclassified information and report the status of their review to the White House, via the Office of Homeland Security, within ninety days.[75]

**Agencies Instructed to Use FOIA Exemptions to Control Disclosure of Information.** The accompanying ISOO and OIP memo included a section titled "sensitive but unclassified information," (SBU), which instructed agencies to safeguard "sensitive information related to America's homeland security"(SHSI), and told them to consider all applicable FOIA exemptions if FOIA

---

[73] (...continued)
Secretary, Department of Defense, *Federal Register*, v. 63, no. 20, Jan. 30, 1998, pp. 4582-4583, referring to 32 CFR part 149 1998;63 FR 4583, Jan. 30, 1998, citing authority as Executive Order 12968 (69 FR 40245, 3 CFR 1995 Comp., p. 391.) The regulation defined SBU as in the Computer Security Act of 1987 as: "Sensitive but Unclassified. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." "Technical Surveillance Countermeasures" was defined as "Techniques and measures to detect and nullify a wide variety of technologies that are used to obtain unauthorized access to classified national security information, restricted data, and/or sensitive but unclassified information."

[74] Section 19.3, Scope, in section 375 DM 19, Department of the Interior, Departmental Manual, effective date: 4/15/02. Available at [http://elips.doi.gov/elips/release/3397.htm].

[75] White Memorandum for the Heads of Executive Departments and Agencies From Andrew H. Card, Jr., The White House, Subject: "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," Mar. 19, 2002. Available at [http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm].

requests are received for such information.[76] The memo urged agencies to consider using specifically FOIA exemptions 2 and 4 when determining whether to categorize information as "sensitive but unclassified." Exemption 2 refers to "(2) internal personnel rules and practices of an agency," while Exemption 4 deals with "trade secrets and commercial or financial information obtained from a person and privileged or confidential." The ISOO/OIP memo cautioned that "The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information." See **Appendix 3** for excerpts of the memo.

As further justification, the memo referred agencies to guidance on FOIA that had been issued by Attorney General Ashcroft in October 2001. This memorandum expressed the Administration's intent to comply with FOIA while, at the same time, instructing agencies, when undertaking discretionary disclosure determinations under FOIA, to consider protecting values and interests to which the Bush Administration is committed, including "safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information, and, not least, preserving personal privacy."[77] In explaining the intent of the memo, the Department of Justice said

> In replacing the predecessor FOIA memorandum, the Ashcroft FOIA Memorandum establishes a new "sound legal basis" standard governing the Department of Justice's decisions on whether to defend agency actions under the FOIA when they are challenged in court. This differs from the "foreseeable harm" standard that was employed under the predecessor memorandum. Under the new standard, agencies should reach the judgment that their use of a FOIA exemption is on sound footing, both factually and legally, whenever they withhold requested information.

In the predecessor memorandum issued by Attorney General Janet Reno in 1993, agencies were encouraged to release documents even if the law provided a way to withhold information, if there was no "foreseeable harm" from doing do. The October 2001 memo underscored the need to ensure that information about agency deliberations not be made public and encouraged agencies to make disclosure determinations under FOIA "only after full and deliberate consideration of the

---

[76] "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Memorandum for Departments and Agencies, From Laura L.S. Kimberly, ISOO, NARA, and Richard L. Huff, and Daniel J. Metcalfe, OIP, Dept. of Justice, Subject; "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Mar. 19, 2002. Available at [http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm].

[77] "New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001. This Department of Justice release includes "Memorandum for Heads of all Federal Departments and Agencies, From: John Ashcroft, Attorney General, Subject: The Freedom of Information Act, Oct. 15, 2001."Available at [http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm]

institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."[78]

Also, referring to the need for heightened sensitivity after the September 2001 terrorist attacks, the October 2001 memo instructed agencies to utilize FOIA exemptions when making an agency "assessment of, or statement regarding, the vulnerability of ... a critical asset ..."[79] or the need to protect critical infrastructure information, referenced in the memo as "critical systems, facilities, stockpiles, and other assets from security breaches and harm — and in some instances from their potential uses weapons of mass destruction in and of themselves. Such protection efforts, of course, must at the same time include the protection of any agency information that could enable someone to succeed in causing the feared harm."[80]

The Attorney General's October 2001 memorandum instructed agencies to interpret FOIA exemption 2 broadly to permit withholding of a document, which if released would allow circumvention of an agency rule, policy or statute, thereby impeding the agency in the conduct of its mission. (This is generally referred to as the high profile interpretation of exemption 2.)[81] It said that agencies should "avail themselves of the full measure of exemption 2's protection for their critical infrastructure information as they continued to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks."[82] The memo referred to guidance that was issued in 1989 describing the sensitivity of vulnerability assessments and the need to exempt such information from disclosure under FOIA.[83]

---

[78] "New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001.

[79] "New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001.

[80] "New Attorney General FOIA Memorandum Issued," Oct. 15, 2001. For additional analysis, see CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security*. For additional explanation of the Administration's objectives in releasing this guidance, see: U.S. Department of Justice, Office of Information and Privacy, *Freedom of Information Act Guide and Privacy Act Overview,* May 2002, ed., pp. 16-17, 124-127.

[81] See U.S. Department of Justice, Office of Information and Privacy, *Freedom of Information Act Guide and Privacy Act Overview,* May 2002, ed., pp. 16-17, 124-127 and "New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001, which hotlinks to other explanatory documents cited.

[82] "New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001.

[83] Excerpts from the 1989 guidance follow: "When processing records for disclosure under the Freedom of Information Act, it is sometimes difficult for FOIA officers to immediately recognize the sensitivity of information warranting protection under the Act's exemptions. One type of record for which that should not be so, however, is a record in which an agency specifically assesses its vulnerability (or that of another institution or installation) to some form of outside interference or other wrongful harm. Indeed, vulnerability assessments can be among the most sensitive records maintained by federal agencies.

Vulnerability assessments generally are designed to ensure the security of an institution or installation by safeguarding against possible interference, circumvention or

(continued...)

Pursuant to the Card memo, and attachments, the information to be covered by the Administration's "sensitive but unclassified" homeland security information seems to include records that deal with the agency, public infrastructure the agency might regulate or monitor, some internal databases (reports, data the agency has collected, maps, etc.), vulnerability assessments, some internal deliberations, and information provided to the government by private firms, such as chemical companies.[84]

Although most of this information is not classified, it appears as if security clearances may be required for access to some SHSI and certain types of SBU information. The National Archives and Records Administration (NARA) included in its *Annual Performance Plan, FY2003,*[85] a goal of training state and local officials in the proper handling of classified and sensitive homeland security information. The document stated that this included the objectives of obtaining Top Secret security clearances for state and local officials who need such clearances to handle classified or sensitive homeland security information, and also of developing "a training program at the state and local level for the proper use and handling of classified and sensitive but unclassified homeland security information for all officials with Top Secret security clearances and other officials who have access to sensitive information. Finally ISOO will ensure that Federal agencies have the necessary classification authority for homeland security information."

It should be noted that, on March 12, 2002, and again on June 23, 2003, the House oversight committee on FOIA, the Committee on Government Reform, called the Attorney General's October 2001 memorandum into question and specifically rejected its standard to allow the withholding of information sought under FOIA whenever there is merely a "sound legal basis" for doing so.[86] The committee

---

[83] (...continued)
unlawful action by outsiders. Typically, a vulnerability assessment first seeks to identify an institution's assets, programs or systems that are deemed to be most sensitive. In so doing, it usually pays particular attention to the ones that are believed to be, for one reason or another, especially vulnerable to external harm. Further, in analyzing an item of identified vulnerability, such an assessment commonly will describe the specific security measures (as well as possible countermeasures) that can be employed to combat that vulnerability.

Thus, by its very nature, a vulnerability assessment necessarily consists of sensitive information that, in the wrong hands, can itself do great harm." ("OIP Guidance: Protecting Vulnerability Assessments Through Application of Exemption Two,"*FOIA Update*, Summer 1989 Available at: [http://www.usdoj.gov/oip/foia_updates/Vol_X_3/page3.html].)

[84] "New Attorney General FOIA Memorandum Issued," Oct. 15, 2001. For additional analysis, see also: CRS Report RL31547, op. cit., and *Freedom of Information Act Guide and Privacy Act Overview,* May 2002, ed., op. cit., pp. 16-17, 124-127.

[85] Submitted to Congress on Feb. 4, 2002. The goal was part of "Long Range Performance Target 2.4, which focused on developing "a uniform sampling system for collecting information about classification activity within the executive branch."

[86] U.S. Congress, House Committee on Government Reform, *A Citizen's Guide on Using the*
(continued...)

directed agencies to withhold documents only in those cases when the agency reasonably foresees that disclosure would be harmful to an interest protected by an exemption.[87]

# Policies for Control of Unclassified Information in P.L. 107-296

## Introduction

The dilemma about balancing security and science is reflected in the Homeland Security Act, P.L. 107-296, signed November 2, 2002. Among other things, it required that research conducted by the Department of Homeland Security (DHS) created by the law "shall be unclassified to the greatest extent possible" (Sec. 306 (a)). Nevertheless, in a signing statement, the President reiterated that the executive branch had the right to implement this provision (and others) in a manner which would protect information "...the disclosure of which could otherwise harm the foreign relations or national security of the United States."[88]

## Protection of Critical Infrastructure Information

P.L. 107-296, also included prohibitions against disclosure under FOIA of "critical infrastructure information" regarding to the security of critical infrastructure and protected systems submitted voluntarily by private companies. Criminal penalties for disclosure by affected employees include fines, dismissal, or imprisonment for up to a year (Section 214).[89] The statute also provided for the preemption of state freedom of information laws regarding the public disclosure of such information if it is shared with a state or local government official in the course of DHS's activities.[90] Subsequently, the Department of Defense issued a memo on March 25, 2003 which applied prohibitions like those in P.L. 107-296 to critical infrastructure information voluntarily submitted to DoD.[91] On April 15, 2003, the Department of Homeland Security published interim rules in the *Federal Register*

---

[86] (...continued)
*Freedom of Information Act and the Privacy Act of 1974 to Request Government Records,* 107th Cong., 2nd sess. H.Rept. 107-371, 2002, p. 3.

[87] H.Rept. 107-371, 2002, op. cit., p. 3. This language is also included in a report with the same title, reported June 23, 2003, in the 108th Congress, 1st sess., H.Rept. 109-172.

[88] [Http://www.whitehouse.gov/news/releases/2002/11/20021125-10.html].

[89] For additional analysis see CRS Report RL31547 *Critical Infrastructure Information Disclosure and Homeland Security*, op. cit.

[90] See also, "Homeland Security Law Contains New Exemption 3 Statute," *FOIA Post,* Jan. 27, 2003.

[91] Memo from H.J. McIntyre on "FOIA Requests for Critical Infrastructure Information," described in Steven Aftergood, "DOD on Critical Infrastructure Info," *Secrecy News*, Apr. 29, 2003 and "Efforts Made to Expand Critical Infrastructure Information," *OMB Watcher, May 5, 2002.*

which implement the critical information infrastructure protection provisions of P.L. 107-296, and which would extend the rules to other agencies by requiring them to pass similar information that they receive to DHS.[92] DHS published a final rule and to established the "Protected Infrastructure Information (PCII) Program on February 18, 2004.[93] The submitted information will be withheld from public disclosure under FOIA and "Initially, the PCII Program Office will limit the sharing of PCII to IIAP [DHS's Information Analysis and Infrastructure Protection Directorate] analysts,"[94] and then, if accepted as appropriate to be safeguarded pursuant to the law and regulations, to other federal agencies. Submitters are to certify, under penalty of fine or imprisonment, that the submitted information is not subject to disclosure under the rules of another department, such as to meet health, safety, or environmental regulations. This later provision is intended to allay some of the fears of groups that suspect companies will submit to DHS information they do not want to be disclosed in order to hide from the public information about pollution, new facilities, or security gaps.

## "Sensitive But Unclassified" Homeland Security Information

P.L. 107-296 also required the President to "prescribe and implement procedures" for federal agencies to, among other things, identify, safeguard, and share with appropriate federal, state, and local agencies "homeland security information that is sensitive but unclassified" (Sec. 892). This is often abbreviated SHSI. "Homeland security information" was defined as

> any information possessed by a Federal, State, or local agency that — (A) relates to the threat of terrorist activity; (B) relates to the ability or prevent, interdict, or disrupt terrorist activity; (C)would improve the identification or investigation of a suspected terrorist or terrorist organization; and (D) would improve the response to a terrorist act (Sec. 892(f)(1)).

The law did not define sensitive or "sensitive but unclassified." It stated that, in sharing sensitive but unclassified information with state and local persons, it is the sense of Congress that the procedures developed to share information that is sensitive but unclassified may include requirements for "entering into nondisclosure agreements with appropriate State and local personnel" (Sec. 892(c)(2)(B)).

---

[92] "6 CFR Part 29, Procedures for Handling Critical Infrastructure Information; Proposed Rule, Department of Homeland Security," *Federal Register*, Apr. 15, 2003, pp. 18523-18529. For additional information, see: CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation,* by John Moteff.

[93] The implementing regulations are contained in the Code of Federal Regulation (6 CFR Part 29). (Source: Department of Homeland Security, "DHS Launches Protected Critical Infrastructure Information Program to Enhance Homeland Security, Facilitate Information Sharing," Press Release, Feb. 18, 2004 and attached information sheet "Protected Critical Infrastructure Information (PCII) Program. See the *Federal Register*, Feb. 20, 2004, pp. 8073-8089.

[94] Press release, Feb. 18, 2004, op. cit.

On July 29, 2003, the President assigned his responsibility to provide such procedural guidance to federal agencies and most other responsibilities of sections 892 and 893 of P.L. 107-296 to the Secretary of the Department of Homeland Security (pursuant to Executive Order 13311).[95] The DHS is developing such guidance; no guidance for identifying and sharing sensitive unclassified homeland security information has been issued as of February 17, 2004, but it is expected to be released within the next several months. Also, DHS is drafting the report on implementation of section 892 of P.L. 107-296, as required by Section 893 of the law.

**Federal Agency Implementation Actions.** After the release of the Ashcroft and Card memos some agencies started to respond to this issue in its broadest sense. Some issued policy statements or rules relating to SBU even before passage of P.L. 107-296 or the issuance of the guidance Congress mandated in the law.

Reportedly, some agencies are increasingly inserting restrictions based on the category "sensitive but unclassified" into contracts for unclassified research negotiated with some universities. This has not only raised questions about whether the term should be better defined before it is more widely used but has caused some universities to object to such clauses and have refused to accept federal contract funds for unclassified research that contain them.[96]

Some agencies have defined "sensitive" information that will be protected from public disclosure or might be exempt from disclosure under FOIA, and have developed procedures to share this information with appropriate officials in federal state and local agencies. Several federal agencies have developed guidance or regulations to define SHSI or SBU and protect it from public release. The Nuclear Regulatory Commission's guidance, which it described as interim pending a final Administration definition for SHSI, was released on April 4, 2002. It includes such things as "plan specific information, generated by NRC, our licensees, or our contractors, that would clearly aid in planning an assault on a facility.... Physical vulnerabilities or weaknesses of nuclear facilities.... Construction details of specific facilities.... Information which clearly would be useful to defeat or breach key barriers at nuclear facilities," and "Information in any type of comment (e.g. plant status report, press release) that provides the current status or configuration of systems and equipment that could be used to determine facility vulnerabilities if used by an adversary."[97]

---

[95] The Executive Order was printed in the *Federal Register,* July 29, 2003, pp. 45149-45150. The President retained responsibility to "ensure that such procedures apply to all agencies of the Federal Government" as specified in P.L. 107-296, Sec. 892(a)(2) and responsibilities given to federal agencies to review and share information sharing systems, as specified in P.L. 107, Sec. 892 (b) (7).

[96] Anne Marie Borrego, "Colleges See More Federal Limits on Research," *The Chronicle of Higher Education,* Nov. 1, 2002.

[97] Found in U.S. Nuclear Regulatory Commission, "Withholding Sensitive Homeland Security Information From the Public," Memorandum [to the Commission Members] From

(continued...)

The U.S. Department of Agriculture issued Regulation 3440-002 on "Control and Protection of 'Sensitive Security Information,' " on January 30, 2003. It said it applied to "...the identification of unclassified but sensitive information as 'Sensitive Security Information,' "....[98] The definition applies generally to facilities, critical infrastructure and cyber-based systems (Sec. 6). This information is to be made available only to individual who have a "need-to-know," and the regulation provided procedures to protect it (Secs. 11 and 12 of the regulation).

Pursuant to the Transportation Security Regulations,[99]DHS's Transportation Security Administration (TSA) has defined the types of information that are categorized as "sensitive security information," (SSI) and to be protected from disclosure and be exempted from FOIA. There are also reports that the TSA has sought to remove unclassified congressional testimony tht was already published, "in which a government contractor described security problems at the Rochester, N.Y. airport" on the grounds that it included "sensitive security information."[100] Reportedly, the testimony was removed from some, but not all, sources. The TSA has defined the types of of information that are SSI and to be protected from disclosure and exempted from FOIA.

Some federal agencies have withdrawn from their websites information they have categorized as SBU and that might prove to be useful to terrorists, but which would appear to be accessible to the public under existing laws such as the Emergency Planning and Community Right-To-Know Act of 1986 (42 U.S.C. 11049), which environmental advocates often cite to obtain information. For instance, reportedly, the Department of Energy "removed environmental impact statements which alerted local communities to potential dangers from nearby nuclear energy plants, as well as information on the transportation of hazardous materials."[101] Reportedly, some agencies may be withholding some information that normally would be made available under FOIA requests.[102] According to one report, the Environmental Protection Agency (EPA) has removed documents from its website and the Defense Department has removed more than 6,000 documents in response

---

[97] (...continued)
William D. Travers, April 4, 2002, COMSECY-02-0015.

[98] U.S. Department of Agriculture. Departmental Regulation 32440-0002, Subject "Control and Protection of 'Sensitive Security Information,' " January 30, 2003. Available at [http://www.usda.gov/directives/filese/dr/DR3440-002.htm] or start at http://www.usda.gov/directives/.

[99] U.S. Department of Transportation, "Civil Aviation Security Rules," *Federal Register,* v. 67, no. 36, Feb. 22, 2002 and 49 C.F.R. 1520.7.

[100] Jeff Stein, "TSA Asks Media to Expunge Public Testimony on Airport Security Problems," *CQ Homeland Security,* Feb. 4, 2004.

[101] Marylaine Block, "Vanishing Act: The U.S. Government's Disappearing Data, *ExLibris,* Dec. 6, 2002.

[102] "Results of OMB Watch FOIA Request on Information Withheld," *OMB Watch,* May 15, 2002, [http://www.ombwatch.org/article/articleview/735/1/104/]. See also, "Researchers Stymied by Block on Government Documents," *CNN.Com,* Oct. 15, 2002.

to the memo.[103] The Nuclear Regulatory Commission is reported to have removed documents from its website.[104] State governments have removed data from public websites, including "hospital security plans and information on energy stockpiles of pharmaceuticals" in Florida.[105] The Secretary of Defense was reported to have said a review of information accessible on DOD websites indicated over 1,500 instances where posted data were insufficiently reviewed for sensitivity or not adequately protected. He said the trend should be reversed and he advised that " 'Thinking about what may be helpful to an adversary prior to posting any information to the web could eliminate many vulnerabilities....' "[106] One critic said in response, "However, such guidance, taken by itself, would dictate the elimination of nearly all accurate information from DoD web sites since practically anything could be of use to an adversary in some conceivable scenario."[107] It has been reported that some information which researchers have sought and that agencies removed from their websites is being advertised to researchers through commercial vendors on CD and hard copy. Some researchers now fear that the deleted information, including USGS topographic map information will "become unavailable due to tighter security .... "[108] This might deny public access to such information of could possibly resulting in a "commercialization of information similar to what happened with Landsat data in the 1980s, when the satellite imagery became privatized, dramatically raising the cost of research."[109]

Some assessments made so far of the changes to agency FOIA procedures based on the Ashcroft October 2001 guidance, which restricted discretionary disclosures under FOIA, indicate that the new policies appear not to have had a major impact on agency activities. Preliminary analysis issued by the National Security Archive regarding implementation of this guidance in 35 agencies indicated that while a few agencies, such as NASA, EPA, and the Departments of the Interior and Navy, had to undertook significant activities to comply, most did not. Some agencies reported that the Card memo, rather than the Ashcroft memo, would appear to have had more significant effects on disclosures requested via FOIA.[110] According to a GAO assessment, released in September 2003, the Ashcroft memo appears to have

---

[103] "The Bush Administration's Secrecy Policy: A Call to Action to Protect Democratic Values," *OMB Watch,* Oct. 25, 2002.

[104] Block, op. cit.

[105] Block, op cit.

[106] Steven Aftergood, "Rumsfeld Wants More Info Off the Web, *Secrecy News,* Jan. 16, 2003.

[107] Steven Aftergood, "Rumsfeld Wants More Info Off the Web, *Secrecy News,* Jan. 16, 2003.

[108] Lisa M. Pinsker, "Science Policy, Mapping Secure Boundaries for Data." *Geotimes,* 2003, at [http://www.geotimes.org/current/NN_data.html].

[109] Pinsker, 2003, op. cit.

[110] See: "The Ashcroft Memo: 'Drastic' Change or 'More Thunder Than Lightning'?, The National Security Archive Freedom of Information Audit, "Preliminary Findings Regarding Implementation of White House Guidance Regarding FOIA," Phase One Presented Mar. 14, 2003, at [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB84/press.htm].

had only limited impact on the processing of FOIA requests. GAO reported that 48% of the FOIA officers surveyed "... did not notice a change with regard to the likelihood of their agencies' making discretionary disclosures. About one third of the FOIA officers reported a decreased likelihood; of these officers, 75 percent cite the new policy as a top factor influencing the change."[111]

In contrast, others have concluded that the effects are serious. For instance, the Lawyers Committee for Human Rights, in a 2003 report, described as an example, DOD refusal to release an unclassified conference report on lessons learned from the 2001 anthrax attacks and concluded "The 'homeland security information' provision represents a sweeping new delegation of authority to expand secrecy well beyond formal classification procedures in a manner that is likely to further impair Congress' oversight responsibilities. Whether Congress will step in to try to mitigate this potential remains uncertain." [112]

Some speculate that less unclassified information will be made available since passage of Section 214 of P.L. 107-296, relating to critical infrastructure information. This has been viewed as a controversial provision. Critics say while it would protect sensitive information submitted to the government about dams, buildings, electric power lines, pipelines, rail transit and so forth. Others say that it "... could make government officials fearful of disclosing information about corporate activities that pose risks to the public."[113] Reportedly, the American Civil Liberties Union (ACLU) was concerned "... that companies could ensure secrecy for a wide range of information provided to the government simply by declaring that it involves critical infrastructure and then demanding confidentiality."[114] It also "contended that the ... law could prevent the disclosure of potential health risks from uranium stored at private sites or of defects in railroad tracks ... [or] ...that the law might discourage whistle-blowers from coming forward with revelations about corporate wrongdoing."[115] Supporters of withholding this kind of information cite the potential threats to homeland security that may be incurred if such information is allowed to remain widely accessible. They say that potential terrorists could use information about critical U.S. public and private infrastructure to design and implement attacks that could destroy U.S. power, communications, transportation

---

[111] U.S. General Accounting Office. *Freedom of Information act, Agency Views on Changes REsulting from New Administration Policy,* Report to the Ranking Minority Member, Committee on the Judiciary, U.S. Senate, Sept. 2003, Highlights page, GAO-03-981.

[112] Lawyers Committee for Human Rights, *Assessing the New Normal: Liberty and Security for the Post-September 11 United States,* 2003, p. 8.

[113] Dan Morgan, "Disclosure Curbs in Homeland Bill Decried: Information From Companies at Issue," *Washington Post,* Nov. 16, 2002, p. A13. See also: Barbara Yuill, "Experts Discuss Privacy Impacts of Newly Signed Homeland Security Act," *Daily Report for Executives,* Dec. 11, 2002. See also: "Reaction to Passage of Homeland Security Bill: All Aboard the Homeland Security Express, Bill Creates Dangerous New FOIA Exemption," *OMB Watch,* Nov. 20, 2002.

[114] Morgan, Nov. 16, 2002.

[115] Morgan op.,cit. See also CRS Report RL31530, *Chemical Plant Security*.

and public works networks and facilities. Access to this kind of information, they say, should be given only to those with a need to know.

## Concerns About Sensitive Information in Non-governmental Research and Scientific Publications

Acknowledging the serious potential threats from release of certain kinds of "sensitive" privately developed research information, professional scientific societies and groups have considered developing ways to regulate, review, identify and deal with publication of "sensitive" journal articles.[116] Some believe that private scientific publishers and editors will feel compelled to model their publications policy for sensitive papers on guidelines that the federal government develops for release of agency documents. There is considerable controversy about this issue.

**National Academies' Policy.** The National Academy of Sciences says it voluntarily deleted from a public version of a report, and put into a separate appendix, certain information on vulnerabilities of U.S. croplands after review by the U.S. Department of Agriculture, the sponsoring agency.[117] The rationale was that terrorists might be able to exploit information on vulnerabilities. The information is being made available "on a need-to-know basis" to a select list of persons including "federal, state, and local government workers, officials involved in homeland security, and animal and plant health scientists, but not members of the media or the general public. Anyone interested in the appendix has to file a written request.... Academy staff members then call applicants, ascertain their identify, and ask why they need the report...."[118] Reportedly, the Academy cited FOIA exemption 2, "which protects matters 'related solely to the internal personnel rules and practices of an agency' " in justifying this procedure.[119] Regarding another Academy report, DoD's Joint Non-Lethal Weapons Directorate reportedly took several months to review a study on non-lethal weapons, finally released in November 2002. But there are "conflicting opinions of that review, including whether it was used improperly to suppress NAS' criticism of DoD's non-lethal weapons program."[120]

---

[116] See, for example, `Richard Monastersky, "Publish and Perish?," *Chronicle of Higher Education*, Oct. 11, 2002 and William J. Broad, "Researchers Say Science Is Hurt by Secrecy Policy Set Up by the White House," *New York Times,* Oct. 19, 2002.

[117] Peg Brickly, "New Antiterrorism Tenets Trouble Scientists," *The Scientist,* Oct. 28, 2002, referring to a Sept. 19, 2002 Academy press release. See also Jeffrey Mervis and Erik Stokstad, "NAS Censors Report on Bioterrorism," *Science,* Sept. 19, 2002.

[118] Martin Enserink, "Science and Security: Entering the Twilight Zone of What Material to Censor," *Science,* Nov. 22, 2002, p. 1548.

[119] Enserink, Nov. 22, 2002, op. cit.

[120] Christopher Castelli, "NAS Study Shows Messy Reality Tied To Balancing Security, Openness," *Inside the Navy*, Dec. 2, 2002.

On October 18, 2002, the three presidents of the National Academies issued a statement[121] which sought to balance security and openness in disseminating scientific information. It summarized the policy dilemma by saying that "Restrictions are clearly needed to safeguard strategic secrets; but openness also is needed to accelerate the progress of technical knowledge and enhance the nation's understanding of potential threats." The statement encouraged the government to reiterate that basic scientific research should not be classified, that nonclassified research reporting should not be restricted, and that vague and poorly defined categories of research information, such as sensitive but unclassified, should not be used. "Experience shows that vague criteria of this kind generate deep uncertainties among both scientists and officials responsible for enforcing regulations. The inevitable effect is to stifle scientific creativity and to weaken national security." The statement outlined "action points" for both government and professional societies to consider when developing a dialogue about procedures to safeguard scientific and technical information which could possibly be of use to potential terrorists.

The National Academies held a workshop on this subject early in 2003[122] in cooperation with the Center for Strategic and International Studies.[123] Reportedly, during this meeting, Administration officials, stated the view that scientists should voluntarily craft a policy that protects sensitive information and that they should assist the government "... to help it identify and censor truly sensitive findings," especially in the biological sciences.[124] One result is that the CSIS and the Academies established a "Roundtable on Scientific Communication and National Security," a working group composed of scientific and security leaders which will hold continuing discussions to try to develop a workable publications policy.[125]

**Other Groups.** Some scientists, including Dr. Ronald Atlas, President of the American Society for Microbiology,[126] have suggested that the scientific community should come together to discuss the issue of balancing secrecy in science and scientific publication in a move similar to the 1975 Asilomar conference, which helped to develop guidelines for information communication and institutional review boards to monitor and control the development of genetically modified organisms. Some suggest that perhaps the National Academy of Sciences or a committee of a

---

[121] "Presidents Statement on Science and Security in an Age of Terrorism, From Bruce Alberts, William A. Wulf, and Harvey Fineberg, Presidents of the National Academies," Oct. 18, 2002. See also, "Background Paper on Science and Security in a Age of Terrorism," issued by the Academies with the statement.

[122] Atlas, op. cit., Oct. 25, 2002.

[123] "The National Academies and CSIS to Host Jan. 9 Meeting On National Security and Scientific Openness," Press release, Dec. 12, 2002, [http://www.national-academies.org/topnews/#tn1212b].

[124] David Malakoff, "Researchers Urged to Self-Censor Sensitive Data," *Science,* Jan. 17, 2003, p. 321.

[125] Malakoff, Jan. 17, 2003, p. 321; Lum, Jan. 21, 2003, op. cit. See also:"Roundtable on Scientific Communication and National Security," A Collaborative Project of the Center for Strategic and International Studies and the National Academies, Charter Statement.

[126] Atlas, Oct. 25, 2002.

relevant professional society be established to evaluate whether parts of methodology of especially sensitive research should be published.[127] Reportedly, Dr. Anthony Fauci, Director of the NIH National Institute of Allergy and Infectious Diseases (NIAID), which is receiving the bulk of funds allocated to NIH for counterterrorism R&D, said on October 3, 2002, that while transparency in publication should be the norm, consideration should be given to developing a "specially appointed committee to determine whether publication is appropriate." He suggested the formation of a panel to determine whether it is appropriate to pursue certain types of biomedical research," similar to the Asilomar Conference.[128] Others have suggested that only certain kinds of sensitive research be restricted or classified, such as research relating to the "weaponization of biological and toxin agents...."[129]

The International Council for Science (ICSU), an international non-governmental scientific association,[130] announced that it will review threats to scientific freedom, including limitations or restrictions being placed on the conduct and communication of scientific information and the freedom of movement of scientific materials.[131] The Council of the American Library Association adopted a resolution at its June 2002 meeting that urged that the provisions relating to "Sensitive but Unclassified" information be dropped from the Card memorandum and that urged "government agencies ... ensure that public access to government information is maintained absent specific compelling and documented national security or public safety concerns."[132] The American Association of University Professors (AAUP) announced on September 11, 2002, that it was creating a committee to review and analyze "post-September 11 developments which impinge on academic freedom."[133]

In January 2004, the American Physical Society (APS) Council released a statement which concluded, "Restricting exchange of scientific information based on non-statutory administrative policies is detrimental to scientific progress and the

---

[127] Daniel S. Greenberg, "Self-Restraint by Scientists Can Avert Federal Intrusion," *Chronicle of Higher Education,* Oct. 11, 2002.

[128] Benjamin Y. Lum, "Security Exceptions to Transparency in Publishing NIH-funded Research Will Be Rare, Fauci Says," *Washington Fax,* Oct. 11, 2002.

[129] Raymond A. Zilinskas and Jonathan B. Tucker, "Limiting the Contribution of the Open Scientific Literature to the Biological Weapons Threat," *Journal of Homeland Security,* Dec. 2002.

[130] ICSU "is a non-governmental organization founded in 1931 to bring together natural scientists in international scientific endeavour. It comprises 101 multi-disciplinary National Scientific Members, Associates and Observers (scientific research councils or science academies) and 27 international, single-discipline Scientific Unions to provide a wide spectrum of scientific expertise enabling members to address major international, interdisciplinary issues which none could handle alone. ICSU also has 24 Scientific Associates." See: [http://www.icsu.org/].

[131] "Freedom in the Conduct of Science: ICSU Examines Current Issues Around the Globe," Public Release, Oct. 10, 2002.

[132] "Actions of the ALA Council, 2002 Annual," June 13-19, 2002, Atlanta, GA.

[133] See [Http://www.aaup.org/newsroom/press.2002/911com.htm].

future health and security of our nation. The APS opposes any such restrictions, such as those based on the label 'sensitive but unclassified'...."[134]

**Professional Groups Views That Scientists Should Voluntarily "Self-Regulate" Research and Publications.** Some professional scientific groups, such as the American Society for Microbiology, have called upon their members to be cautious about releasing or publishing information which might be useful to potential terrorists, including specifically the "methodology" sections of some scientific papers, and have established publication review committees to evaluate the sensitivity of articles presented for publication in their journals.[135] The society has established procedures to have an editorial panel review for sensitivity manuscripts which deal with "select agents." So far, reportedly only one paper has been asked to be revised.[136]

In February 2003, shortly after the Academies/CSIS 2003 meeting, 32 journal editors and scientists, including officials with the American Association for the Advancement of Science and the American Society of Microbiology, issued a statement on "Statement on Scientific Publications and Security," published in *Science*, *Nature* and the *Proceedings of the National Academy of Sciences*, saying that they would take security issues into account when reviewing research papers for publication. Each scientific publication will develop its own process to review papers submitted for publication.[137]

A National Academy of Sciences report, entitled *Biotechnology Research in an Age of Terrorism: Confronting the "Dual Use" Dilemma*, published in 2003 and dubbed the "Fink" report for its chairman, called for greater self-regulation by scientists, using institutional biosafety committees at academic and research institutions, for research that could possibly aid terrorists. It also urged creation of a new federal National Science Advisory Board for Biodefense to provide guidance to nongovernmental researchers. But it did not propose government control of such research.[138]

---

[134] American Physical Society, "Council 'Deplores Restriction of Non-Classified Scientific Information," *APS News Online*, Jan. 2004, available at [http://www.aps./org/apsnews/0104/010403.html].

[135] Ronald M. Atlas, "National Security and the Biological Research Community," *Science*, Oct. 25, 2002..

[136] Benjamin Y. Lum, "Journal Editors Caution Against Overly Restrictive Policies Based on Security," *Washington Fax*, Jan. 21, 2003.

[137] Alan Boyle, "Science Journals Join Bioterror Fight," *MSNBC News*, Feb. 15, 2003. For the statement, entitled "Statement on Scientific Publication and Security," see, www.sciencemag.org, Feb. 21, 2003; for a list of signatories, see: [http://www.sciencemag.org/feature/data/secuirty/authors.shtml].

[138] The report is available at www.nap.edu/catalog/10827.html. See also, David Malakoff and Martin Enserink, "Researchers Await Government Response to Self-Regulation Plea," *Science*, Oct. 17, 2003, pp. 368-369.

Partly in reaction, the American Association of University Professors (AAUP) Special Committee on Academic Freedom and National Security in a Time of Crisis, in a report issued in 2003, urged a note of caution regarding self-restraint by the scientific community: "the academic community must be careful not to impose on itself a regulatory burden that differs from the government's only in the locus of administration."[139] Although there has been no evidence of negative effects on scientific research so far, " a realistic appraisal of what the scientific community is doing to monitor its own members requires us to be aware of the possibility that researchers and journal editors might exercise their responsibilities with too much rigor and thus inadvertently give too little attention to freedom's needs."[140]

**Policy Options.** Congress has also expressed interest in this topic. Shortly after publication on July 1, 2002, in *Science* magazine online, of a controversial scientific paper that described the synthesis of an infectious polio virus from mail order components, Congressman Weldon introduced H.Res. 514 (107th Congress). It expressed "serious concern" about the paper, which was funded by the Defense Advanced Research Projects Agency (DARPA), and called for tighter controls on the publication of certain scientific research. It also sought to have the scientific community and the executive branch ensure that information that may be used by terrorists is not made widely available, or is properly classified.[141] The resolution was not reported from the committee.

For additional information see CRS Report RL31695, *Balancing Scientific Publication and National Security Concerns: Issues for Congress.*

---

[139] AAUP, *Academic Freedom and National Security in a Time of Crisis,* Section III. 2003, available at [http://www.aaup.org/statements/REPORTS/911report.htm].

[140] AAUP, *Academic Freedom and National Security in a Time of Crisis,* Section III. 2003, available at [http://www.aaup.org/statements/REPORTS/911report.htm].

[141] See *Congressional Record,* July 26, 2002.

# Policy Issues About "Sensitive But Unclassified" Information

## Introduction

As explained above, some federal agencies use the definition of "sensitive" in the Computer Security Act of 1987 as the basis for identifying information to label SBU. Other agencies have expanded the definition of sensitive in various ways, with some agencies including information exempt from release under FOIA and others including other kinds of information determined to be sensitive to a particular agency's activities. Following the terrorist attacks of September 11, 2001, the Administration instructed agencies to withhold more information when undertaking discretionary disclosure deliberations under FOIA. Agencies were instructed to balance access to information with the needs to protect critical infrastructure information, national security, law enforcement effectiveness, agency deliberations and decision-making, and related values and interests, and to use specifically FOIA exemptions 2 and 4. When making such deliberations, they were also told to consider, on a case by case basis, "benefits that result from the open and efficient exchange of scientific, technical, and like information."

These actions have raised significant policy issues, such as allegations that the terms sensitive and SBU are ambiguous because they are subject to agency interpretation. This, some say, makes it difficult to identify and safeguard such information, while raising questions about the need for uniformity in standards. Some say expanded interpretation of FOIA exemptions 2 and 4 to identify SBU divides those who want increased security of information from those who want public access to the information now exempted in order to protect public and community oversight, civil liberties, and accountability, to promote the conduct of science, or to monitor private sector activities. The procedures mandated in P.L. 107-296 are intended to guide agencies toward the use of similar procedures to identify, share, and safeguard sensitive but unclassifed homeland security information. As will be discussed below, there has been considerable debate about this content of these proposed guidelines.

## Historical Controversy About "Sensitive But Unclassified"

Even before the terrorist attacks of 2001, there had been considerable controversy about the meaning and use of the term SBU. One position is that agencies should interpret the term more broadly to categorize and safeguard more information as SBU; alternatively, others say that this category is often imprecise and leads to indiscriminate withholding of information from the public.

For instance, a February 28, 1994 report, *Redefining Security*, by the Joint Security Commission prepared for the Director of the CIA and the Secretary of Defense, which according to the Federation of American Scientists (FAS) "was the first significant post-cold war examination of government security policies and

practices,"[142] estimated that as much as 75% of all government-held information may be sensitive and unclassified. It recommended that more attention should be paid to protecting such information and labeling it as SBU within the defense, intelligence and other sectors of government as well as "... information that, while neither classified nor government-held, is crucial to U.S. security in its broadest sense." Continuing, it said,

> We have in mind information about, and contained in, our air traffic control system, the social security system, the banking, credit, and stock market systems, the telephone and communications networks, and the power grids and pipeline networks. All of these are highly automated systems that require appropriate security measures to protect confidentiality, integrity and availability."[143]

In a contrasting position, the aforementioned Moynihan commission report, entitled *Report of the Commission on Protecting and Reducing Government Secrecy, 1997*, noted that agencies often use different types of mandates to justify protecting unclassified information and these range from the very broad to specific. This causes problems because

> "... [V]irtually any agency employee can decide which information is to be so regulated;" there is no oversight of this categorization and agencies control access "though a need-to know process," and "... the very lack of consistency from one agency to another contributes to confusion about why this information is to be protected and how it is to be handled. These designations sometimes are mistaken for a fourth classification levels, causing unclassified information with these markings to be treated like classified information."[144]

As a result, the Commission concluded that more information is protected than is warranted.

An attempt had been made in December 1994, the report said, to develop a policy to address sensitive but unclassified information, but it "met with great resistance by both the civilian side of the Government and industry" because the process was controlled by the Security Policy Board, which dealt largely with classified information and was controlled by the defense and intelligence community.[145] The report also found that overzealous labeling of information as

---

[142] Section on "Dealing with Sensitive but Unclassified Information," *Redefining Security*, Feb. 28, 1994, [http://www.fas.org/sgp/library/jsc/].

[143] See, [http://www.fas.org/sgp/library/jsc/].

[144] *Report of the Commission on Protecting and Reducing Government Secrecy, 1997*, op. cit.

[145] *Chap.* V. *Information Age Insecurity*, in *Report of the Commission on Protecting and Reducing Government Secrecy, 1997*, op. cit. The board was created by Presidential decision directive 29 issued by President Clinton in September 1994 and abolished on April 24, 2001, pursuant to National Security Presidential Directive 1 [http://www.fas.org/sgp/spb/].

SBU could be avoided if more attention were devoted to improving the security of government computer-information systems[146] to prevent unauthorized access.

Critiquing the wide scope of the current DOE definition of SBU (see above under the section, "Department of Energy"), a Center for Strategic and International Studies (CSIS) commission dealing with DOE laboratories reported in 2002:

> The Department's official definition is so broad as to be unusable. ...There is no ... common understanding of how to control ... [SBU] ..., no meaningful way to control it that is consistent with its level of sensitivity, and no agreement on what significance it has for U.S. national security. Sensitive unclassified information is causing acute problems at DOE. ... Security professionals find it difficult to design clear standards for protection. Scientists feel vulnerable to violating rules on categories that are ill defined. Without clear definition or standards for protection, those who oversee implementation for the Department find it extremely difficult to measure laboratory performance.
>
> ... Yet the Department tends to treat this information as if subject to security measures not unlike those for classified information. It is considered when developing background checks for foreign visitors and when reviewing presentations that may involve sensitive unclassified information.
>
> ... The lack of management discipline around sensitive unclassified information both hinders the scientific enterprise and reduces the ability of security and counterintelligence professionals to control information where necessary.[147]

The CSIS commission recommended that DOE avoid using the definition and label "SBU." "By avoiding these labels," it said, "the Department can depart from treating unclassified information as if subject to national security controls. The Department should have just three classes of information: (1) classified; (2) unclassified but subject to administrative controls; and (3) unclassified, publicly releasable."[148] DOE should also avoid use of a sensitive subjects list or change its name, since the list deals primarily with items and technology potentially subject to export control.[149] "If information is not classified but requires administrative control," DOE should consider using "the category of information designated official use only (OUO)...." "A single office within DOE administers OUO, which has guidelines established in law and unclassified information could be reviewed for applicability under the OUO statutes. Existing statutes governing certain types of

---

[146] Chap. II, section on "Enhancing Congressional Oversight and Policy Formulation" of *Report of the Commission on Protecting and Reducing Government Secrecy, 1997*, op. cit.

[147] Commission on Science and Security, John J. Hamre, chairman, *Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories*, Apr. 2002, Washington, D.C., Center for Strategic and International Studies, pp. 55-56.

[148] *Science and Security in the 21st Century,* op. cit., p. 62.

[149] *Science and Security in the 21st Century:* op. cit., p. 62.

sensitive unclassified information could remain unchanged and distinct from OUO (i.e. unclassified but controlled nuclear information [UCNI]), as long as they provide sufficiently clear guidelines for control."[150]

During the 107th Congress, congressional interest in this topic was reflected in a recommendation made by the congressional Joint Inquiry Into September 11, which among other things recommended a review encompassing the concepts of sensitive or classified information:

> Congress should also review the statutes, policies and procedures that govern the national security classification of intelligence information and its protection from unauthorized disclosure. Among other matters, Congress should consider the degree to which excessive classification has been used in the past and the extent to which the emerging threat environment has greatly increased the need for real-time sharing of sensitive information. The Director of National Intelligence, in consultation with the Secretary of Defense, the Secretary of State, the Secretary of Homeland Security, and the Attorney General, should review and report to the House and Senate Intelligence Committees on proposals for a new and more realistic approach to the processes and structures that have governed the designation of sensitive and classified information. The report should include proposals to protect against the use of the classification process as a shield to protect agency self-interest.[151]

## Critiques of the White House (Card) Memorandum

While many observers agree with the objectives and implementation of the March 2002 Card memorandum in order to lessen potential terrorist attacks, some critics have urged caution in interpreting it and the accompanying guidance which appears to allow agencies to widen types of information to be exempt from disclosure under FOIA. It has been argued that "Several of the new restrictions on information are not congruent with the existing legal framework defined by the Freedom of Information Act (FOIA) or with the executive order [Executive Order 12598] that governs National Security classification and declassification."[152] Some have questioned the authority of national security directives pertaining to "sensitive, but unclassified" information or say that where Congress has statutorily prescribed policy contrary to information management policy prescribed in presidential directives or agency regulations, the supremacy of statutory law would seemingly prevail. One

---

[150] *Science and Security in the 21st Century*, op. cit., p. 57. OUO information is defined: "A designation identifying certain unclassified by sensitive information that may be exempt from public release under the Freedom of Information Act. Source: DOE 471.2A, Information Security Program, 3-27-97 and Draft DOE Glossary." from [http://labs.ucop.edu/internet/security/brief00/#Anchor-SECURITY-3800].

[151] Recommendations of the Final Report of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence Joint Inquiry into the Terrorist Attacks of September 11, 2001, Dec. 10, 2002. Available at [http://intelligence.senate.gov/pubs107.htm].

[152] Steven Aftergood and Henry Kelly, "Making Sense of Information Restrictions After September 11," *FAS Public Interest Report*, Mar./Apr. 2002.

critic of the March 2002 White House memo cautioned that the term "sensitive but unclassified" may be "the most dangerous level of secrecy, because it was not defined [in the past] and there were no channels of appeal."[153] Similarly, others say that "... no administrative mechanisms have been developed to allow those who disagree with the decision to withhold information to challenge the decision or to seek some remedy to the decision. To make this policy work, the federal government needs to develop procedures that will allow citizens the ability to disagree with the conclusions of the agency denying or withholding the information."[154]

## Policy Options for "Sensitive But Unclassified" Information

Some who seek to clarify policies for controlling public or private scientific information that is not classified believe that scientific progress and innovation, and even the fight against terrorism, will be harmed by limiting information flow. Yet these critics share the goal of trying to keep potential terrorists from obtaining information that could be used to threaten the United States. Some have called for closer cooperation between the scientific and intelligence community to draft guidelines relating to safeguarding scientific information that might be useful to potential terrorists.[155] These conflicting objectives raise perplexing dilemmas for policymakers and scientists alike. Policy options discussed below focus on several parts of this debate, including establishing uniformity in definitions and implementing guidelines; establishing an appeals process for SBU information; and the potential to classify or label as SBU more research information.

**Considerations Related to a Uniform Definition of SBU.** Since agencies define the term SBU differently, various interpretations could lead to the possibility that information that should not be released to the public because of its potential value to terrorists might be released; that agencies might not release SBU information to other agencies, or to state or local officials; or that the public may be denied access to information whose release might be permitted. Questions about ambiguities in the definition of the term SBU may raise interest about legislating, or overseeing the process of developing, uniform criteria for SBU, especially since, in P.L. 107-296, Congress encouraged nonfederal first responders to safeguard such information via nondisclosure agreements.[156]

In order help set standards for SBU and SHSI, and to resolve policy dilemmas surrounding definitions and procedural controls, after release of the Card

---

[153] "Science and Technology: Secrets and Lives; Academic Freedom," *The Economist,* Mar. 9, 2002.

[154] Laura Gordon-Murnane, "Access to Government Information in a Post 9/11 World," *Searcher,* June 1, 2002.

[155] See, for instance, James B. Petro and David A. Relman, "Understanding Threats to Scientific Openness," *Science,* Dec. 12, 2003, p. 1898.

[156] For an assessment of these issues, see: "Sensitive But Unclassified Provisions in the Homeland Security Act of 2002," June 11, 2003, *OMB Watch.*

memorandum in March 2002, the White House Office of Homeland Security was reported to have drafted a definition for SHSI,[157] and that "originally, there was an initiative to issue a Presidential Directive on unclassified but Homeland Security-sensitive information."[158] This was never publically released, but several agencies, including the Nuclear Regulatory Commission, utilized it when developing criteria to define SHSI as discussed in the Card and Ashcroft memos.[159] Subsequently the Office of Homeland Security asked the White House Office of Science and Technology Policy (OSTP) and the Office of Management and Budget to develop guidance, which had been expected to be released in 2002 or 2003. An objective of the proposed guidance was to withhold information from persons who should not have access to it, but to allow such information to be shared with those who might have a need for it, such as law enforcement and emergency response personnel.[160]

OMB and OSTP met with stakeholder groups, including academics and scientists, to obtain their views about how to develop guidance.[161] During a meeting held in late August 2002, with academic and scientific officials and others discussing the March 2002 memos, their implementation, and definitions, "[a]cademic and scientific representatives ... argued [that] basic and applied research, even research performed by the government, should not be subject to [sensitive but unclassified homeland security information] SHSI guidelines and advocated following existing rules for the handling of sensitive information, such as the Centers for Disease

---

[157] Discussed in U.S. Nuclear Regulatory Commission, "Withholding Sensitive Homeland Security Information From the Public," Memorandum [to the Commission Members] From William D. Travers, April 4, 2002, COMSECY-02-0015.

[158] "Challenges in Disseminating Homeland Security Information," Discussion with Steve Cooper, Special Assistant to the President and Senior Director for Information Integration, White HOuse Office of Homeland Security, *CENDI Participants and Alternates Meeting Minutes,* Oct. 22, 2002, available at [http://www.dtic.mil/cendi/minutes/pa_1002.html].

[159] COMSECY-02-0015, op. cit.

[160] Statement of Hon. John H. Marburger, Director, Office of Science and Technology Policy Before the Committee on Science, Oct. 10, 2002. Dr. Marburger said, OHS asked OMB to develop guidance for Federal agencies "to ensure consistency of treatment of this information within the government and by recipients, such as first responders. See also: "OMB Tackles Sensitive But Unclassified Information," *Secrecy News,* Sept. 3,2002. Daniel J. Chenok, is the OMB official cited as explaining that OMB was developing guidance and that an objective was to permit the sharing of information with first responders.

[161] See: "Challenges in Disseminating Homeland Security Information," Discussion with Steve Cooper, Special Assistant to the President and Senior Director for Information Integration, White House Office of Homeland Security, *CENDI Participants and Alternates Meeting Minutes,* Oct. 22, 2002, available at [http://www.dtic.mil/cendi/minutes/pa_1002.html]; "Sensitive but Unclassified," *OMB Watch,* Sept. 3, 2002. See also Statement of Hon. John H. Marburger, Director, Office of Science and Technology Policy Before the Committee on Science, Oct. 10, 2002; "OMB Tackles Sensitive But Unclassified Information," *Secrecy News,* Sept. 3,2002; and "Remarks by Secretary Ridge tot he Association of American Universities," *DHS Press Release.* Apr. 14, 2003.

Control and Prevention (CDC) guidance for the handling of select agents."[162] Academic officials reportedly left the meeting convinced that the March memo applied only to "information that was generated and owned by the government, and not university research," nor to university research funded by federal government grants.[163] During hearings on *Conducting Research During the War on Terrorism: Balancing Openness and Security,* held by the House Science Committee on October 10, 2002, White House Office of Science and Technology (OSTP) Director John Marburger testified that the Administration wants "to ensure an open scientific environment" while maintaining homeland security. He said SHSI would apply to federal intelligence, law enforcement and public health information that generally is not made public, but would not necessarily include research results.[164] Several other witnesses endorsed this position.

According to OSTP Director Marburger, SBU information related to homeland security "... may be withheld from public disclosure only when it warrants protection under one of the nine exceptions of the Freedom of Information Act."[165] The relationship between FOIA and the Administration's homeland security information policies was the theme of a conference held by the Department of Justice's Office of Information and Privacy for FOIA officers during June 25, 2004.[166] The topics of the meeting were summarized in a *FOIA Post* article, but the discussion summaries were not released to the public.

Despite many meetings in 2002 and 2003 with various stakeholders and apparent attempts to draft policy, no SBU or SHSI policy guidance was issued.

Before July 2003, the OMB/OSTP guidance had been expected to constitute the President's instructions to federal agencies to "prescribe and implement procedures" to "identify and safeguard sensitive homeland security information that is sensitive but unclassified," and to share this information with other federal agencies and appropriate State and local personnel, as required by section 892 (a) (1) (A)(B) of P.L. 107-296. The Secretary of DHS was assigned these functions pursuant to Executive Order 13311, July 29, 2003 and the DHS Office of General Counsel is developing the guidelines mandated by P.L. 107-296. It is not known

---

[162] Lum, op. cit., Oct. 11, 2002.

[163] Anne Marie Borrego, "White House Gets Input from Universities As It Drafts New Rules on Disclosure of Some Sensitive Research," *Chronicle of Higher Education,* Aug. 23, 2002.

[164] For reports on the hearing, see: Anne Marine Borrego, "In Testimony, University Officials Reject 'Sensitive' Designation for Scientific Research," *Chronicle of Higher Education,* Oct. 11, 2002, "Impact of Homeland Security on Research and Education," *FYI, American Institute of Physics Bulletin of Science Policy News,* Oct. 18, 2002, and Cheryl Bolen, "Panel Considers Difficult Balance Between Open Research, Security," *Daily Report for Executives,* Oct. 11, 2002.

[165] Answer to question Q5, in "Answers to Post-Hearing Questions," Responses by Dr., John H. Marburger, Director, OSTP [before the House Science Committee, 2002], available at [http://commdocs.house.gov/committees/science/hsy82178.000/hsy82178_1.HTM].

[166] "FOIA Officers Conference Held on Homeland Security," *FOIA Post,* 2003, available at [http://www.usdoj.gov/oip/foiapost/2003foiapost25.htm].

which perspectives will be used in guidance to federal agencies — the limited definition of sensitive as in the Computer Security Act of 1987, the more expansive, but somewhat limited, conceptualization of SBU in the Card memorandum and attachments, or the broader conceptualization of SBU used by the Department of Energy. It is expected that the definition will extend beyond SHSI *per se*, that is, beyond information not routinely released to the public, such as law enforcement data, personnel information, and information on computer vulnerabilities, to include also a conceptualization of SBU information that could extend to some kinds of scientific and technical data.

Some have speculated that the delay in issuing guidance is due to disagreement about whether there should be public comment — which might involve discussions raised by critics relating to ensuring allowing public access to information that could be used to continue to permit public and community oversight of governmental and industrial activities. Another concern that might be raised by the public in commenting on proposed regulations could focus on penalties for violating nondisclosure agreements that might affect unsuspecting recipients of SBU information.[167] Others say the delay "... may be ... a recognition of the voluntary restraints the academic community has imposed on itself," referring specifically to professional groups' activities in support of voluntary self-restraint[168] for sensitive scientific information. Although the law does not require public comment, an OMB official[169] and a Department of Justice release had said that SHSI guidance would be subject to public notice comment before the regulation was implemented.[170] It is not clear whether the Department of Homeland Security will seek public comment now that it has been given responsibility to draft the regulations.[171] Over 75 public groups, "representing journalists, scientists, librarians, environmental groups, privacy advocates, and others" wrote to DHS Secretary in August 2003, urging that he allow public input on procedures to be prescribed and implemented for identifying,

---

[167] See: "Groups Demand Pubic Input in Writing 'Sensitive But Unclassified' Procedures," *OMB Watch,* Aug. 27, 2003 and letter sent by these groups to DHS Secretary Tom Ridge on Aug. 27, 2003. In the letter to Secretary Ridge, the groups alleged that the procedures develop "would prohibit public disclosure of information subject o agreements between the government and those receiving ;sensitive but unclassified' information. One recent analysis estimates that roughly four million people — including pubic health officials not employed by government at any level — could be asked ...to sign formal nondisclosure agreements. Those agreement s would be enforceable through civil and criminal sanction."

[168] AAUP, *Academic Freedom and National Security in a Time of Crisis,* Section III. 2003, available at [http://www.aaup.org/statements/REPORTS/911report.htm].

[169] Interview with OMB official, May 29, 2003.

[170] "FOIA Officers Conference Held on Homeland Security," *FOIA Post,* 2003, available at [http://www/usdoj.gov/oip/foiapost/2003foiapost25.htm].

[171] *Sharing &Protecting Homeland Security Information: Avoiding Conflict Between the Media and the Government: A Panel Discussion Made Possible by the Annenberg Public Policy center With a grant from the Robert Wood Johnson Foundation,* National Press Club, Washington, D.C., June 11, 2003, p. 5.

safeguarding, and sharing the sensitive but unclassified homeland security information referenced in section 892.[172]

**Factors Agencies Might Use in Developing Nondisclosure Policy for SBU Information.** The Card and Ashcroft memos, together with section 892 of P.L. 107-296, have given agencies a basis to make decisions about restricting access to certain electronic and hard copy information that previously may have been accessible to the public, but whose continued distribution might be detrimental to homeland security. But it is unclear what conceptualizations agencies and the DHS guidance will use. As noted above, agencies have discretion to identify and withhold from the public, as sensitive or as sensitive but unclassified, information which they determine is subject to nondisclosure (pursuant to both the Computer Security Act of 1987 and the Administration's interpretation of FOIA). Since the basis of these determinations is subject to interpretation, both agency program managers and the public who might seek access to such information may confront ambiguity in definitions and different kinds of balancing tests. There are questions about the uniformity of definitions used by different agencies and which values or objectives should be encompassed in a risk analysis on which such nondisclosure determinations might be based.

The definition of what information is SBU, at a minimum, is likely to encompass concepts which are defined as sensitive in the Computer Security Act 1987, that is to protect information whose disclosure "could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under ... the Privacy Act." Also, it may encompass the NIST criteria for sensitive information protection: confidentiality, integrity, and availability.[173] Additionally, among the topics the Administration instructed agencies to consider when making "discretionary disclosures" of SBU homeland security-related information that could be exempt from FOIA is the "need to protect critical systems, facilities, stockpiles, and other assets from security breaches and harm — and in some instances from their potential use as weapons of mass destruction in and of themselves."[174] The Administration also stressed that agencies, when applying exemption 2, should consider the needs for an informed citizenry to ensure accountability, "safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information, and not least preserving personal privacy."[175] Also to be considered were " ... benefits that

---

[172] See: "Groups Demand Pubic Input in Writing 'Sensitive But Unclassified' Procedures," *OMB Watch,* Aug. 27, 2003; "IRE [Investigative Reporters and Editors] Supports Public Comments on Homeland Security Information Sharing Act," Aug. 19, 2003, available at [http://www.ire.org/foi/sharingact.html].

[173] CSL Bulletin: "Advising Users on Computer System Technology," Nov. 1992. [http://nsi.org/Library/Compsec/sensitiv.txt.]. (Emphasis added.)

[174] *Freedom of Information Act Guide and Privacy Act Overview, May 2002, edition,* op. cit., p. 17, with the discussion based on Ashcroft memorandum of Oct. 15, 2001 and White House Card Memorandum of March 19, 2002.

[175] *Freedom of Information Act Guide and Privacy Act Overview, May 2002, edition,* op. cit., pp. 16-17 with the discussion based on Ashcroft memorandum of Oct. 15, 2001 and White

(continued...)

result from the open and efficient exchange of scientific, technical, and like information." Criteria for sensitive but unclassified SHSI also are likely to reference the types of information P.L. 107-296 identifies as "homeland security information" — "any information possessed by a Federal, state, or local agency that — relates to the threat of terrorist activity; relates to the ability to prevent, interdict, or disrupt terrorist activity; would improve the identification or investigation of a suspected terrorist or terrorist organization, or would improve the response to a terrorist act" (Sec. 892 (f)).

Because of the difficulty of balancing the needs for information with security, some critics of the White House March 2002 memo have focused on the need for developing guiding principles. According to Steven Aftergood and Henry Kelly, "In deciding how to treat such information, the administration should enunciate a clear set of principles, as well as an equitable procedure for implementing them and appealing adverse decisions," with the appeals procedure "outside the originating agency."[176] They said that "The guiding principles could be formulated as a set of questions, such as:

> Is the information otherwise available in public domain? (Or can it be readily deduced from first principles?) If the answer is yes, then there is no valid reason to withhold it, and doing so would undercut the credibility of official information policy.
>
> Is there specific reason to believe the information could be used by terrorists? Are there countervailing considerations that would militate in favor of disclosure, i.e., could it be used for beneficial purposes? Documents that describe in detail how anthrax spores could be milled and coated so as to maximize their dissemination presumptively pose a threat to national security and should be withdrawn from the public domain. But not every document that has the word "anthrax" in the title is sensitive. And even documents that are in some ways sensitive might nevertheless serve to inform medical research and emergency planning and might therefore be properly disclosed.
>
> Is there specific reason to believe the information should be public knowledge? It is in the nature of our political system that it functions in response to public concern and controversy. Environmental hazards, defective products, and risky corporate practices only tend to find their solution, if at all, following a thorough public airing. Withholding controversial information from the public means short-circuiting the political process, and risking a net loss in security.

Given the contending values and factors that affect a workable definition and implementing rules, Congress may monitor the guidance that DHS develops to assist agencies in identifying sensitive homeland security information and SBU. Because of the potential implications of the forthcoming DHS concepts for private scientific

---

[175] (...continued)
House Card Memorandum of March 19, 2002.

[176] Aftergood and Kelly, Mar./Apr. 2002, op. cit.

publications policy, various constituencies and scientific groups will undoubtedly seek to examine the balance between security and access to information in these guidelines.

**The Potential to Classify More Research Information.** Several activities have occurred recently that might increase the amount of scientific research information that is classified. As noted above, NSDD 189 and Executive Order 12958 both prohibit classification of certain kinds of federal scientific research information except for reasons of national security. NSDD 189 deals with basic research and Executive Order 12958 applies the prohibition to fundamental, or what it defines as basic and applied, research. Recently, the heads of several federal agencies with substantial research responsibilities, who did not have classification authority under Executive Order 12958, the prevailing executive order on classifying information,[177] were given original classification authority. These include the Secretaries of Health and Human Services[178] and of Agriculture,[179] and also the Administrator of the Environmental Protection Agency.[180] Some of the agencies with new classification authority, especially Health and Human Services and Agriculture, support substantial amounts of counterterrorism research, as well as of fundamental research in a variety of scientific and technical areas, often performed on an extramural basis by researchers in colleges and universities.[181]

New Executive Order 13292, issued on March 25, 2003, amends Executive Order 12958 on classified national security information. The amendment permits classification of "scientific, technological, or economic matters relating to the national security, *which includes defense against transnational terrorism*" (new clause in italics, sec. 1.4 (e)). The amendment appears to highlight that national security-related scientific, technological, and economic information dealing with defense against international terrorism may be classified. Given that the definition of "national security," in the two executive orders is not changed and that definition could have encompassed matters related to transnational terrorism, it is unclear if the amended order widens the scope of scientific, technological, and economic information to be classified.[182]

---

[177] A new executive order on classification was issued on March 25, 2003. See: "Executive Order 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information," White House Press Release, Mar. 25, 2003.

[178] "Order of December 10, 2001 — Designation Under Executive Order 12958, *Federal Register,* Dec. 12, 2001, Volume 66, Number 239, pp. 64345-64347.

[179] "Order of September 26, 2002 — Designation Under Executive Order 12958," *Federal Register,* Sept. 30, 2002, Volume 67, Number 189, pp. 61463-61465.

[180] "Order of May 6, 2002 — Designation Under Executive Order 12958," *Federal Register,* May 9, 2002, Volume 67, Number 90, p. 31109.

[181] See CRS Issue Brief IB10088, *Federal Research and Development: Budgeting and Priority-Setting Issues, 108th Congress,* and CRS Report RS21270, *Homeland Security and Counterterrorism Research and Development: Funding, Organization, and Oversight.*

[182] The definition of "national security" is the same in both executive orders. It reads: "National security means the national defense or foreign relations of the United States."

In addition, the Department of Defense reportedly plans to reissue its guidelines relating to pre-publication review of extramural research that it funds outside of its own laboratories. Recently several university groups wrote a letter to the Director of the Office of Science and Technology Policy complaining that more agency program officials are inserting pre-publication review clauses into contracts, including for fundamental research, without explanation as to their justification. This has a "pernicious effects," they said, "not only with regard to the freedom to publish but also with regard to employment of foreign-born students and researchers on federally funded research projects. If the contract clauses require blanket screening of any and all foreign-born scientists, universities will object."[183]

Agencies which recently were given original classification authority are now developing implementing guidelines and appointing security officers in operating units. Given the long-standing federal policy embodied in Executive Order 12598 and in NSDD 189 of not classifying basic scientific research, except if release would threaten national security, the balance between science and security in agency guidelines will remain a topic of interest and concern. Interest in this topic may be heightened because of the recent changes made in Executive Order 13292 to the definition of the kinds of scientific, technological, and economic information that may be classified.

The scientific and academic communities are expected to pay close attention to these issues. Among the questions that may be raised are:

- Will new controls be placed on federally funded research, including both intramural research conducted in an agency's laboratories, and on extramural research, that might be federally funded but conducted in nonfederal academic and industrial research laboratories?
- Will controls encompass both classification levels and use of designations such as sensitive and sensitive but unclassified?
- Will designation of a controlled research project be made before the award of funds and the start of a project, or after a project is completed and during a pre-publication review phase?
- What kinds of requirements will be placed upon nonfederal researchers to safeguard research information?
- How will such controls affect the conduct of academic research for the federal government?
- How will such controls differ from the controls on proprietary research information that are deemed acceptable by most academic institutions eager to receive financial support from industry?
- Will research agencies with original classification authority modify their long-standing policies of encouraging publication and dissemination of federally funded research results?

---

[183] "AAU/COGR/NASULGC Letter to OSTP Director on Scientific Openness," Jan. 31, 2003, from President, Association of American Universities, President, National Association of State Universities and Land-Grant Colleges, and President, Council on Governmental Relations, [http://www.aau.edu/research/Ltr1.31.03.html].

- Under the expanded definition of scientific and technological information subject to classification in Executive Order 13292, will agencies classify information that might have otherwise been categorized as SBU?

**Appeals Process for SBU Information.** Another continuing issue is expected to be an appeals process for designating information as SBU. Stephen Aftergood, with the Federation of American Scientists (FAS), suggested that " ... An appeals panel that is outside of the originating agency and that therefore does not have [the] same bureaucratic interests at stake would significantly enhance the credibility of the deliberative process. The efficacy of such an appeals process has been repeatedly demonstrated by an executive branch body called the Interagency Security Classification Appeals Panel (ISCAP)."[184] Another suggested approach is that "To solve disputes that develop out of the new category of 'sensitive but unclassified' information, one could allow the Information Security Oversight Office (a part of the Executive Branch) to receive appeals to review disputes and challenges to executive agency decisions regarding the release of documents and reports The Office would oversee the appeals, it would have another set of eyes that would examine the requested information and review it in a different context that the executive agency. The ISOO might be able to work with both the agency involved and those requesting the information to reach a compromise that everyone could accept. It would also have the effect of keeping the oversight of the information in the hands of the executive branch."[185]

**Determination of "Tiered" Access to SBU Information.** Some agencies have discussed developing procedures to permit "tiered," or selective, access to qualified and pre-screened individuals for some scientific and technical information, that could be categorized as SBU or SHSI. Reportedly, EPA requires researchers to obtain sponsorship from a senior EPA official, have their requests approved in advance and register before using the Envirofacts database.[186] EPA also has issued instructions to utilities to submit threat or vulnerability assessments to the agency. Using a protocol issued in December 2002, reportedly, EPA "... will keep sensitive information in the assessments secure. The documents will be kept in one location under lock and only individuals designated by EPA will have access to them."[187] EPA also will release other agency information to selected individuals only in hard copy at EPA offices and libraries throughout the nation.[188] The Federal Energy Regulatory Commission (FERC) issued a final rule, effective April 2, 2003,

---

[184] Steven Aftergood, "Making Sense of Government Information Restrictions," *Issues in Science and Technology,* Summer 2002.

[185] Gordon-Murnane, op. cit., June 1, 2002.

[186] Mary Graham, "The Information Wars," *The Atlantic Monthly,* Sept. 2002, pp. 36-38.

[187] "EPA Issues Instructions to Utilities on Submitting Threat Assessments," *Daily Report for Executives,* Jan,. 8, 2003, p. A-24.

[188] See, for instance, Meredith Preston, "Researchers Says Work May Be Impeded By Restrictions on Environmental Database," *Daily Report for Executives,* Mar. 28, 2002. See also CRS Report RL31354, *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education.*

which limits release of its critical energy infrastructure information on a selective or "tiered" basis to members of the public based on their need to know and the legitimacy of their need as determined by the Commission.[189] FERC said it would not alter its responsibilities under FOIA, but appears to be broadening, or at a minimum, reinterpreting implementation of exemptions to disclosure under FOIA.[190] The U.S. Geological Survey has announced that it will implement four levels of control for its information products:

> a. No sensitivity is determined. No restriction is required. b. Product is determined to be sensitive. Do not distribute. c. Sensitivity has been determined for a previously distributed product that is widely available. Withdrawal would be ineffective. Continue distribution of current version. Restrict distribution of new features to updates for 1 year. d. Product is restricted according to directive from another agency with specific authority for public safety or national security.[191]

The equity of procedures for "tiered" or selective access; the need to create public and or private panels to examine controls on the release of some information; and the need to clarify relationships between the private sector and the government with respect to safeguarding information in scientific publications to protect the public interest are issues which may be raised in the legislative context.

---

[189] "Critical Energy Infrastructure Information," Federal Energy Regulatory Commission Final Rule, *Federal Register*: Mar. 3, 2003, pp. 9857-9873 and "Amendments to Conform Regulations With Order No. 630 (Critical Energy Infrastructure Information Final Rule) Notice of Proposed Rulemaking, Federal Energy Regulatory Commission," *Federal Register,* Apr. 16, 2003, pages 185638-18544.

[190] "FERC Rulemaking to Restrict Information Access," *OMB Watch,* Sept. 16, 2002.

[191] Gordon-Murnane, op. cit.

# APPENDICES

## Appendix 1. History of Atomic Energy "Restricted Data" Controls

The development and history of atomic energy restricted data controls were explained in a document prepared in 1989 by Arvin S. Quist, a classification officer at the Oak Ridge Gaseous Diffusion Plant, Oak Ridge National Laboratory, which is operated on contract for the Department of Energy.[192] Excerpts below from the Quist document explain the relevant provisions of these laws.

> In the ... Atomic Energy Act of 1946, Congress established a special category of information called "Restricted Data." *Restricted Data was defined to encompass "all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power."*[193] Thus, by operation of law, nearly all atomic (nuclear) energy information fell within the definition of RD. The Atomic Energy Act authorized the AEC to control the dissemination of RD, specifying as a prerequisite to access to this information that an individual must have a security clearance ....
>
> ... Two particularly unique and significant aspects of RD warrant emphasis. First, a positive action is not required to put information into the RD category. If information falls within the Act's definition of RD, it is in this category from the moment of its origination; that is, it is "born classified." The government has no power to determine that information is RD ... only the power to declassify RD. [In practice, the Government (Department of Energy) determines whether information falls within the definition of Restricted Data.] ... The "born classified" concept is unique with RD. This concept assumes that newly discovered atomic energy information might be so significant with respect to the nation's security that it requires immediate and absolute control. ...National Security Information is not so designated until an original classifier makes a positive determination that the information falls within the definition of NSI ....
>
> Although RD is said to be born classified, the Atomic Energy Act does not specifically designate it as "classified" information. The Act defines RD and prescribes very strict methods for its control without stating that it is "classified" information. However, the Act does describe declassification of RD; therefore, by implication, RD is "classified." A second unique aspect of RD is that information does not have to be owned or controlled by the government to be classified as RD. ... The circumstance could even arise in which an individual could originate RD and then not be allowed to possess it because of lack of security clearance or "need to know." The Atomic Energy Act does not forbid an individual

---

[192] Source: Arvin S. Quist, [Classification Officer, Oak Ridge Gaseous Diffusion Plant Oak Ridge National Laboratory], *Security Classification of Information, Volume 1. Introduction, History, and Adverse Impacts,* Prepared by the Oak Ridge Gaseous Diffusion Plant, Oak Ridge, Tennessee 37831-7101, operated by Martin Marietta Energy Systems, Inc. for the U.S. Department of Energy, under contract DE-AC05-84OR21400, Prepared Sept. 1989, K/CG-1077/V1.

[193] Emphasis added.

> to generate RD, but, once RD is generated, the Act prohibits its communication to persons not authorized to receive it.

In 1951, Congress amended the Atomic Energy Act of 1946 to make certain atomic energy information available to other countries for purposes of weapons development, but the National Security Council had to approve these information flows. The Atomic Energy Act of 1954 amended the 1946 act to include "an increased emphasis on wider dissemination of atomic energy information, to make more of it accessible to U.S. industry and to the world in order to permit the development of nuclear reactors for commercial production of electric power ... as a consequence of President Eisenhower's [1953] Atoms For Peace initiative ...." The Quist document says:

> With respect to the control of information, the 1954 Act stated:
>
> "It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. Consistent with such policy the Commission shall be guided by the following principles:
>
> (a) Until effective and enforceable international safeguards against the use of atomic energy for destructive purposes have been established by an international arrangement, there shall be no exchange of Restricted Data with other nations except as authorized by section 2164 of this title; and
>
> (b) The dissemination of scientific and technical information relating to atomic energy should be permitted and encouraged so as to provide that free interchange of ideas and criticism which is essential to scientific and industrial progress and public understanding and to enlarge the fund of technical information. ...[42 U.S.C. sec. 2161.]"
>
> ... The 1954 Act added "industrial progress," "public understanding," and "enlarge the fund of technical information" as reasons to disseminate atomic energy information. Those additions provided the basis for the subsequent declassification or downgrading of much atomic energy information.
>
> ... The 1946 Act had permitted declassification of RD only when the AEC determined that it could be published without "adversely affecting the common defense and security .... The 1954 Act changed "adversely affecting" to "undue risk," thereby shifting the balancing test towards declassification of more information .... The increased emphasis of the 1954 Act in disseminating atomic energy information is further exemplified by a continuous review requirement...:
>
> ... Prior to the Atomic Energy Act of 1954, private persons could not have access to RD for commercial purposes (e.g., development of commercial nuclear power reactors). The only reason for allowing private persons to have access to such data was on a need-to- know basis, in connection with national defense work. Although the 1954 Act envisioned the commercial development of nuclear energy, the Act contained no express provisions permitting access to RD for commercial purposes. This hurdle was overcome in 1956 when the AEC used its administrative powers to establish an Access Permit Program ... Under this program, a permitted is able to have access to RD "applicable to civil uses of atomic energy for use in his business, trade or profession."

# Appendix 2. Foreign Affairs Manual on SBU Information[194]

12 FAM 540, SENSITIVE BUT UNCLASSIFIED INFORMATION (SBU) *(TL:DS-61; 10-01-1999)*
12 FAM 541 SCOPE *(TL:DS-46; 05-26-1995)*
a. SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act.
b. SBU information includes, but is not limited to:
(1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and
(2) Information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers.

12 FAM 542 IMPLEMENTATION *(TL:DS-46; 05-26-1995)*
Previous regulations regarding LOU material are superseded and LOU becomes SBU as of the date of this publication.

12 FAM 543 ACCESS, DISSEMINATION, AND RELEASE *(TL:DS-61; 10-01-1999)*
a. U.S. citizen direct-hire supervisory employees are responsible for access, dissemination, and release of SBU material. Employees will limit access to protect SBU information from unintended public disclosure.
b. Employees may circulate SBU material to others, including Foreign Service nationals, to carry out an official U.S. Government function if not otherwise prohibited by law, regulation, or interagency agreement.
c. SBU information is not required to be marked, but should carry a distribution restriction to make the recipient aware of specific controls. To protect SBU information stored or processed on automated information systems, the requirements found in 12 FAM 600 (Information Security Technology) must be met.

12 FAM 544 SBU HANDLING PROCEDURES: TRANSMISSION, MAILING, SAFEGUARDING/STORAGE, AND DESTRUCTION *(TL:DS-47; 06-08-1995)*
a. Regardless of method, transmission of SBU information should be effected through means that limit the potential for unauthorized public disclosure. Since information transmitted over unencrypted electronic links such as telephones may be intercepted by unintended recipients, custodians of SBU information should decide whether specific information warrants a higher level of protection accorded by a secure fax, phone, or other encrypted means of communication.
b. SBU information may be sent via the U.S. Postal Service, APO, commercial messenger, or unclassified registered pouch, provided it is packaged in a way that does not disclose its contents or the fact that it is SBU.
c. During nonduty hours, SBU information must be secured within a locked office or suite, or secured in a locked container.

---

[194] Source is: [http://foia.state.gov/docs/12fam/12m0540.pdf].

d. Destroy SBU documents by shredding or burning, or by other methods consistent with law or regulation.

12 FAM 545 RESPONSIBILITIES *(TL:DS-46; 05-26-1995)*
Unauthorized disclosure of SBU information may result in criminal and/or civil penalties. Supervisors may take disciplinary action, as appropriate. State offices responsible for the protection of records are outlined in 5 FAM. See 3 FAM for regulations and process on disciplinary actions. (12 FAM 550 provisions regarding incidents/violations do not pertain to SBU.)

## Appendix 3. Excerpts From ISOO/OIP Guidance, March 18, 2002[195]

III. Sensitive But Unclassified Information

In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958. The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.

All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions. See *FOIA Post*, "New Attorney General FOIA Memorandum Issued" (posted 10/15/01) (found at www.usdoj.gov/oip/foiapost/2001foiapost19.htm), which discusses and provides electronic links to further guidance on the authority available under Exemption 2 of the FOIA, 5 U.S.C. § 552 (b)(2), for the protection of sensitive critical infrastructure information. In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552 (b)(4).

As the accompanying memorandum from the Assistant to the President and Chief of Staff indicates, federal departments and agencies should not hesitate to consult with the Office of Information and Privacy, either with general anticipatory questions or on a case-by-case basis as particular matters arise, regarding any FOIA-related homeland security issue. Likewise, they should consult with the Information Security Oversight Office on any matter pertaining to the classification,

---

[195] Source: "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Memorandum for Departments and Agencies, From Laura L.S. Kimberly, Information Security Oversight Office, National Archives and Records Administration, and Richard L. Huff, and Daniel J. Metcalfe, Office of Information and Privacy, Dept. of Justice, Subject; "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," March 19, 2002.

declassification, or reclassification of information regarding the development or use of weapons of mass destruction, or with the Department of Energy's Office of Security if the information concerns nuclear or radiological weapons.