Order Code RL33303

CRS Report for Congress
Received through the CRS Web

"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information

February 15, 2006

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

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 FEB 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library and Knowledge Repository Defense Acquisition University Fort Belvoir, VA**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**86**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

"Sensitive But Unclassified"Information and Other Controls: Policy and Options for Scientific and Technical Information

Summary

Providing access to scientific and technical information for legitimate uses while protecting it from potential terrorists is complex and poses difficult policy choices. Federally funded, extramural academic research (basic and applied) is supposed to be "classified" if it poses a security threat; otherwise, it is to be "unrestricted." Since the September 11, 2001 terrorist attacks, controls increasingly have been placed on some types of unclassified research and scientific and technical information, including information used to inform decision making and citizen oversight. These controls include "sensitive but unclassified" (SBU) labels; restrictive contract clauses; visa controls; controlled laboratories; and the widening of legal restrictions on access to some federal biological, transportation, critical infrastructure, geospatial, environmental impact, and nuclear information. On December 16, 2005, President Bush instructed federal agencies to standardize procedures to designate, mark, and handle SBU information, and to forward recommendations for government-wide standards to the Director of National Intelligence (DNI). Federal agencies do not use uniform definitions of SBU information or have consistent policies for safeguarding or releasing it. This lack of uniformity and consistency raises issues about how to identify SBU information, especially scientific and technical information; how to keep it from those who would use it malevolently, while allowing access for those who need to use it; and how to develop uniform nondisclosure policies and penalties.

This issue also involves implementation of the Freedom of Information Act (FOIA). Following the 2001 terrorist attacks, the Bush Administration issued guidance that reversed the previous Administration's "presumption of disclosure" approach to releasing information under FOIA and cautioned agencies to consider withholding SBU information if there was a "sound legal basis" to do so. Some agencies say that information labeled SBU is exempt from disclosure under FOIA, even though such information per se is not exempt under FOIA. In addition, the 2002 enactment of the Federal Information Security Management Act (FISMA), P.L. 107-347, rendered moot the definition of SBU that some agencies had used since the passage of the Computer Security Act of 1987, P.L. 100-235, which identified sensitive information by content. FISMA requires all agencies to categorize the criticality and sensitivity of all information, not just sensitive information, according to three security control objectives — confidentiality, integrity, and availability of information — across a range of risk levels and to use safeguards based on risk of release. Many federal agencies have not yet fully implemented these new procedures.

Several actions and proposals have been made to reconcile differences related to these issues are: to standardize concepts of "sensitive" information (P.L. 109-90, H.R. 2331); to modify penalties for disclosure (S. 494, S. 888, H.R. 1317, H.R. 3097); to clarify FOIA (S. 394, S. 589, S. 622, S. 1181, S. 1873, H.R. 867, and H.R. 1620); to widen the use of risk-based approaches to information control; to centralize review, handling, and appeals processes; and to evaluate the impact of federal policies on nongovernmental professional groups' prepublication review and self-policing of sensitive research. This report will be updated as necessary.

Contents

"Sensitive But Unclassified"Information and Other Controls: Policy and Options for Scientific and Technical Information

Introduction to the Issues

Federal agencies have long confronted the need to balance the release of information for public use with the need to withhold information that could be used to threaten privacy or security. The term "sensitive but unclassified" (SBU) information was used before the terrorist attacks of September 11, 2001, even though there was (and is) no statutory definition for it. Since 9/11 more agencies have started to use the term "SBU," or some variant of it, and to implement security systems to identify and protect nonclassified information whose release might benefit terrorists. Many questions have been raised about how to design uniform policies and controls for SBU information. This report focuses on controls for two kinds of scientific and technical information — information used in research and scientific publication and information used to serve broader public policy purposes, such as in regulatory decisionmaking and citizen oversight. Both public and privately controlled information are included and in some respects, private professional groups' responses are being defined by public pressures and decisions.

Two divergent perspectives are discernable. From one perspective, broadening controls to deny public access to federal SBU information will constrain terrorists, who might use it to threaten buildings, infrastructure, people, and services. It has been estimated that "our adversaries derive up to 80% of their intelligence from open-source information."[1] Another source put this at 90%, referring to information about local energy infrastructures, water reservoirs, dams, highly enriched uranium storage sites, and nuclear and gas facilities. Moreover, some say that the potential for terrorism is heightened if terrorists can aggregate seemingly innocuous bits of public information.[2] Although many agencies have begun to limit public access to sensitive information, from this perspective, these efforts are inadequate.

In contrast to those who seek to widen controls, another view contends that inadequate and insufficient sharing of information with the public and among first responders potentially weakens efforts to protect the nation from terrorist attacks. A related perspective is that as government policy on sharing information shifts to the

---

[1] In a document issued by the Pacific Northwest National Laboratory, a Department of Energy affiliated national laboratory, in "F.A.Q. Mozart," at [http://www.pnl.gov/isrc /mozart/faq.html.]

[2] Greg Griffin, "Program Management Perspective: Sensitive Unclassified Information," *The Dragon's Breath*, April 2003.

"need to know" rationale that has become more prevalent since the 9/11 terrorist attacks, the imposition of more controls will deny ordinary citizens information relating to research, environmental protection, transportation, and so forth that they need in order to be informed[3] and to hold accountable government and industry decisionmakers. Some say new control policies unduly limit access to information needed to advance the progress of science and technology and the development of technologies to counter threats, arguing that if scientific and technical information needs to be restricted, it should be classified.

This report traces the evolution of SBU-related controls; summarizes actions taken to protect certain types of scientific and technical information; describes critiques of some control policies; and summarizes proposals and actions, including congressional, executive and other initiatives, to clarify these issues and develop policies that serve various stakeholders. It also raises issues that may warrant further attention.[4]

Summary of Federal Policies to Classify or Control Scientific and Technical Information

Generally, pursuant to National Security Decision Directive 189 (NSDD-189), fundamental (basic or applied) research conducted in universities is not to be labeled "classified" if does not affect national security; it is therefore "unrestricted."[5] Nevertheless, as one commentator noted, "[T]he federal government seems to

---

[3] The *Final Report of the National Commission on Terrorist Attacks Upon the United States*, July 22, 2004, (also called *The 9/11 Commission Report*) encouraged the promotion of a "need- to-share" culture, as opposed to a "need-to-know" culture of information protection, focusing on the development of a "trusted information network" to make information more accessible. (Available at [http://www.9-11commission.gov/report/911Report.pdf].)

[4] This report updates CRS Report RL31845, *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, by Genevieve J. Knezo, which described the history of governmental controls on "sensitive unclassified information."

[5] National Security Decision Directive-189 (NSDD-189), titled "National Policy on the Transfer of Scientific, Technical and Engineering Information" and issued on Sept. 21, 1985, says that 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, "... to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy ... 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." "Fundamental research" is defined as "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community...." This policy is reflected in Executive Order 12958. NSDD-189 is still in effect, as stated in a letter from the National Security Advisor to the Center for Strategic and International Studies (Issued by National Security Advisor Condoleezza Rice on November 1, 2001).

possess wide latitude in declaring information, even purely scientific research, classified or at least sensitive to prevent publication."[6]

Policies for Classification of Research Information

If research does compromise national security, it may be classified pursuant to Executive Order 12958 and Executive Order 13292 — the latter of which expanded the government's ability to classify some scientific and technical information to include information related to "defense against transnational terrorism" (Section 1.4 of Executive Order 13292).[7] During 2001 and 2002, the heads of several federal agencies with substantial research responsibilities, who did not have classification authority under Executive Order 12958, were given original classification authority. These included the Secretaries of Health and Human Services[8] and of Agriculture,[9] the Administrator of the Environmental Protection Agency,[10] and the Director of the White House Office of Science and Technology Policy (OSTP).[11] Also, pursuant to Executive Order 12958, federally funded researchers at any research-performing institution, including universities and colleges, are obligated to report to the government information that they produce that should be classified.[12] In addition, the

---

[6] Alexander J. Breeding, *Sensitive But Unclassified Information: A Threat to Physical Security*, SANS Institute, 2003, p. 24.

[7] Executive Order 12958, Apr. 17, 1995 (*Federal Register*, 60 FR 19825), 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." Executive Order 13292, Mar. 25, 2003, changed section 1.5 of Executive Order 12958 to permit classification of "scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism" (Sec. 1.4 (e) of Executive Order 13292, *Federal Register*, Mar. 25, 2003). The amendment also added a new category of information, concerning "weapons of mass destruction," which may be classified (Sec. 1.4 (h)). The exemption for basic scientific research not clearly related to national security remains (new Section 1.7).

[8] "Order of December 10, 2001 — Designation Under Executive Order 12958, *Federal Register*, Dec. 12, 2001, Vol. 66, No. 239, pp. 64345-64347.

[9] "Order of September 26, 2002 — Designation Under Executive Order 12958," *Federal Register*, Sept. 30, 2002, Vol. 67, No. 189, pp. 61463-61465.

[10] "Order of May 6, 2002 — Designation Under Executive Order 12958," *Federal Register*, May 9, 2002, Vol. 67, No. 90, p. 31109.

[11] "Order of September 17, 2003 — Designation Under Executive Order 12958," *Federal Register*, Sept. 17, 2003, Vol. 68, No. 184, p. 55257.

[12] "Most government grants for unclassified technical activity specify that if the grantee believes the results of the work warrant classification, the grantee has the responsibility to limit the dissemination of that work and to contact the appropriate U.S. government agency with the authority to classify it. In such extraordinary cases, the initiative to seek classification rests with the grantee, not the government" (*Security Controls on Scientific Information and the Conduct of Scientific Research: A White Paper of the Commission on Scientific Communication and National Security*, Washington, D.C., Center for Strategic and International Studies, June 2005, pp. 5-6). For instance, according to section 850 of the current version of the *NSF Grant Policy Manual*, NSF-02-151, July 2002, "Some basic

(continued...)

government may exercise prepublication reviews on some R&D information,[13] and by writing into contracts control clauses for SBU or classified information. Some R&D information is "born classified," according to the Atomic Energy Act of 1946.[14] In addition, pursuant to the Information Security Act of 1951, certain patent information may be classified if release would harm national security.[15]

Controls on Nonclassified Academic and Industrial Research

Academic and industrial researchers are also subject to sensitive information controls for nonclassified information. For instance, the issue of federal agency research contracts with universities imposing prepublication review clauses was addressed in an April 2004 report, *Restrictions on Research Awards: Troublesome Clauses*, released by the Association of American Universities, in cooperation with

---

[12] (...continued)
research information concerning, among other things, scientific, technological or economic matters relating to the national security or cryptology may require classification. There may be cases when an NSF grantee originates information during the course of an NSF-supported project that the grantee believes requires classification under E.O. 12958. In such a case, the grantee has the responsibility to promptly 1. Submit the information directly to the government agency with appropriate subject matter interest and classification authority or, if uncertain as to which agency should receive the information, to the Director of the Information Security Oversight Office, GSA; 2. Protect the information as though it were classified until the grantee is informed that the information does not require classification, but not longer than 30 days after receipt by the agency with subject matter interest or by the GSA; and 3. Notify the appropriate NSF program Officer." The authority has to decide within 30 days whether to classify the information, and if it requires classification, the "performing organization may wish or need to discontinue the project." Dissemination of findings may also be controlled.

[13] The federal government exercises "prepublication 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 information. The Defense Department (DOD) typically includes "prepublication review" clauses in government contracts for extramural research. 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. Beginning in 1980, all academic cryptography research is to be submitted on a voluntary basis for pre-publication review to the National Security Agency. The U.S. government may enter into contracts to purchase exclusive rights to commercial satellite imagery and may stop the collection and dissemination of commercial satellite imagery for national security reasons. (For additional information, see CRS Report RL31845, op. cit. and CSIS, *Security Controls on Scientific Information*, June 2005, op. cit., pp. 13-14.)

[14] See CRS Report RL31845, op. cit.

[15] Pursuant to 35 U.S.C. 181-188. See CRS Report RL31845 for additional information. According to *OMBWatch*'s report, *Secrecy Report Card 2005: Quantitative Indicators of Secrecy in the Federal Government*, a report by Open the Government.Org. Americans for Less Secrecy, More Democracy, Washington, D.C., 2005, the number of secrecy orders imposed on new patents rose from 83 in 2001 to 124 in 2004, and the number of secrecy orders in effect increased from 4,736 in 2001 to 4,885 in 2004 (p. 5) However, it is likely that most of these were recommended by, and issued to, federal agencies for their own government-owned technical information.

the Council on Government Relations. It detailed 138 instances of restrictions placed on publications or other prohibitions on foreign nationals as preconditions for receiving research awards. The report opposed the practice, recommended that federal agencies adhere to the mandates of NSDD-189, and concluded that governmental restrictions were not compatible with university research.

Export and Visa Controls. Export control regulations generally do not apply to the conduct of fundamental research as long as it is ordinarily published and shared broadly within the scientific community. However, export control regulations and International Traffic in Arms Control regulations (ITAR) permit the government to require licensing for the export, or "deemed export," of certain scientific and technical information to specific foreign countries or citizens of those countries working in the United States[16] on university campuses or in industrial laboratories. During 2004 and 2005, considerable controversy arose[17] over the publication of two

---

[16] 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 give agencies authority to regulate the export of technical data. ITAR controls the release of defense articles specified on the U.S. Munitions List (22 CFR 121) and technical data directly related to them. EAR, among other things, controls 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. 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. Fundamental research, but not all activities related to the conduct of such 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. 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. Nevertheless, there has been considerable ambiguity and confusion regarding these provisions 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 that is used to identify technologies requiring export licensing. The Export Administration regulations categorize as "deemed exports" communications both to foreign nationals about technologies characterized as "sensitive" and to countries identified as "sensitive" under EAR rules. Under language in a rule issued in March 2002, the State Department exempted U.S. universities from obtaining ITAR licenses for export of certain 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, and 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. In addition, collaborators in approved countries would have to guarantee that researchers from non-approved countries were not receiving restricted information. (For sources and additional information, see CRS Report RL31845, op. cit.)

[17] "Controls on 'Deemed Export' May Threaten Research," *Secrecy News*, May 2, 2005.

Inspector General reports,[18] one from the Department of Defense (DOD) and the other from the Department of Commerce (DOC). They proposed strict adherence to government interpretations that, even if the research being conducted is fundamental, the operation, technical training, installation, maintenance, repair, overhaul, or refurbishing of commercially available equipment used in the research is a "deemed export" that requires an export license for certain foreign researchers. This would be for equipment as common as fermenters and global positioning system (GPS) locators and would apply to students from China, Russia, India, and other countries on lists of countries that pose national security threats. In a notice of a proposed rule published in the *Federal Register* on March 28, 2005,[19] the DOC recommended that country of birth rather than of citizenship or permanent residence be used as the criterion for determining nationality for deemed export controls. Subsequently, in January 2006, a DOC spokesman said that because of comments received on the proposed rule, DOC would base controls not on country of birth, but on a foreign national's most recent country of citizenship or permanent residency.[20] DOD's proposed rules were published in July 2005.[21] Final rules are pending as of the publication date of this report.

Some university officials argue that expanded interpretations of rules for "deemed export" licenses may be unnecessary.[22] Other members of the academic community cite problems in administering use controls, including ambiguity about identifying which equipment or material in university laboratories is subject to export controls; discrimination on the basis of nationality; difficulty in controlling access of students and researchers in university laboratories; time required to obtain licenses and inflexibility in obtaining licenses;[23] modest security benefits; slowing or preventing important discoveries due to licensing delays; loss of research talent if

---

[18] U.S. Department of Commerce, Office of Inspector General, *Bureau of Industry and Security, Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the U.S., Final Inspection Report No. OPE-16176,* March 2004, 54 p. *Interagency Review of Foreign Nationals Access to Export-Controlled Technology in the United States, Vol. 1,* April 2004, Report D-20004-062, 33 p.

[19] "Revision and Clarification of Deemed Export Related Regulatory Requirements," Advanced Notice of Proposed Rulemaking, *Federal Register,* Mar. 28, 2005, vol. 70, no. 58, pp. 15607-15609.

[20] Statement of Peter Lichtenbaum, Assistant Secretary of Commerce for Export Adminstration at a conference at the National Academies at which the author of this report was present. See also Kelly Field, Commerce Department Will Drop Some But Not All Restrictions on Foreign Researchers, Colleges Are Told, *Chronicle of Higher Education,* Jan. 17, 2006.

[21] "Defense Federal Acquisition Regulation Supplement: Export-Controlled Information and Technology, Proposed Rule With Request for Comments, *Federal Register*, July 12, 2005, vol. 70, no. 132, p. 39977.

[22] *Security Controls on Scientific Information,* June 2005, op. cit., p. 7.

[23] For instance, see rationale detailed in CSIS, *Security Controls on Scientific Information,* June 2005, op. cit. pp. 9-12, and American Civil Liberties Union, *Science Under Siege: The Bush Administration's Assault on Academic Freedom and Scientific Inquiry,* Written by Tania Simoncelli with Jay Stanley, June 2005, 35 p., which also summarizes reports and the views of the academic community, pp. 9-13.

students and researchers study in other countries; and reduction in research at the leading edge of science.

The three presidents of the National Academies [of Science, Engineering, and the Institute of Medicine] opposed such controls in a letter to DOC Secretary Carlos M. Guitierrez, June 16, 2005, and made several recommendations, including the proposal to "[c]lear international students and postdoctoral fellows for access to controlled equipment when their visas are issued or shortly thereafter so that their admission to a university academic program is coupled with their access to use of export controlled equipment." One policy group recommended an alternative approach: to require a deemed export license for "transfers of technology to specifically identified individuals if specific adverse information exists about that individual."[24] In a 2005 report prepared at congressional request, a National Academies panel recommended providing all foreign students and researchers engaged in fundamental research with access comparable to that provided to U.S. citizens and permanent residents and to remove "... all technology items (information and equipment) from the deemed-export technology lists that are available for purchase on the overseas open market from foreign or US companies or that have manuals that are available in the public domain, in libraries, over the Internet, or from manufacturers."[25] The National Foreign Trade Council and other related technology groups also have opposed these rules.[26] Others charge universities would have to pay "... millions of dollars to inventory sensitive equipment, determine students' birthplaces and study which foreigners were using which machines."[27]

As for other controls to deter terrorism, more governmental scrutiny has been used to review and issue visas for foreign researchers and students, and more items have been placed on the Technology Alert List (TAL), which is now classified. The State Department uses the TAL to identify academic and technical subjects that are viewed as sensitive; foreign students proposing to study these subject undergo extra visa scrutiny under the Visas Mantis program.[28] The State Department also has tightened entry/exit registration of foreign students and scholars and tracks their activities in an effort to deter terrorism. These actions may have prohibited the entry of potential terrorists, but some critics allege that they have reduced the number of

---

[24] CSIS, *Security Controls on Scientific Information*, June 2005, op. cit , p. 12.

[25] The National Academies, *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future*, Executive Summary, 2005, p. 6. See also reports of NAS workshops in May and Sept. 2005, Eugene Russo, "DoD Export Controls Rule Should Not Apply to Fundamental Research, Officials Say," *Research Policy Alert*, Sept. 23, 2005; "National Academies, Societies Criticize on DoD's Proposed Export Control Rule," *Research Policy Alert*, Oct. 18, 2005.

[26] Danielle Belopotosky, "Techies Challenge Planned Changes On 'Deemed Exports,'" *Technology Daily*, June 24, 2005.

[27] Scott Shane. "Universities Say New Rules Could Hurt U.S. Research," *New York Times*, Nov. 26, 2005.

[28] *Science Under Siege*, op. cit., pp. 14-15.

foreign students studying in the United States[29] and increased the number of foreign students studying in other countries.[30]

In 2004, the federal government proposed rules declaring that American scientists could not collaborate with, and American publishers could not edit works authored by, scientists in nations that are targets of trade embargoes, including Iran, Sudan, Libya, Cuba, and North Korea. Most scientific societies opposed these proposals[31] on the grounds that they reduced the intellectual freedom of those in other countries and hampered international science. Subsequently, the administering agency, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), decided to permit editing and peer review, but continued to prohibit collaboration between U.S. scholars and researchers in a sanctioned country.[32]

Policies To Control SBU Information

The history through 2002 of using the label SBU was described in detail in CRS Report RL31845 and is summarized briefly in this section, which also updates action through February 15, 2006.

Introduction to the Term "SBU"

Federal agencies began to use the term "SBU" in the 1970s,[33] but the term has never been defined in statutory law. Starting in 1987 and continuing today, when using the term "sensitive information," some agencies refer to the definition for sensitive information that was used in the Computer Security Act of 1987, P.L. 100-235,[34] and to information exempt from disclosure in the Freedom of Information Act (FOIA)[35] and the Privacy Act, as amended.[36]

---

[29] Molly Laas, "Senate Science Committee to Consider Easing Immigration For Foreign Students," *Research Policy Alert,* Nov. 21, 2005; Marjorie J. Censer, "Visa Problems May Damage U.S. Science, Groups Warn," *American Association of University Professors,* Sept./Oct. 2004. See also: U.S. GAO, *Border Security: Streamlined Visas Mantis Program Has Lowered Burden on Foreign Science Students and Scholars, but Further Refinements Needed,* GAO-05-198, Feb. 2005.

[30] *Science Under Siege*, op. cit., pp. 16-20 and Alison Abbott, "Europe Revamps Visa Rules to Attract World's Best Minds," *Nature,* Oct. 27, 2005. See also American Association of University Professors, *Report by Special Committee on Academic Freedom and National Security in a Time of Crisis,* Nov./Dec. 2003.

[31] One that did not is the American Institute of Aeronautics and Astronautics. See Yudhijit Bhattacharjee, "Society Bars Papers From Iranian Authors," *Science,* June 17, 2005.

[32] *Science Under Siege*, op. cit., pp. 10-11, and Yudhijit Bhattacharjee, "Scientific Publishing: Editing No Longer Infringes U.S. Trade Sanctions," *Science,* Dec. 24, 2004.

[33] Interview with CRS specialist Harold Relyea, December 2005.

[34] 101 Stat. 1724-1730, 40 U.S.C 1441.

[35] 5 U.S.C. 552, as amended by P.L. 104-231, 110 Stat. 3048.

[36] The Privacy Act of 1974, 5 U.S.C. Section 552a , as amended.

Computer Security Act Definition of "Sensitive"

The Computer Security Act of 1987 (CSA) was intended to protect the security and privacy of sensitive unclassified information in federal computer systems and the systems themselves. P.L. 100-235 defined the term "sensitive" information 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).

Because P.L. 100-235 applied to "sensitive information" that was not classified, some say it defined "sensitive but unclassified." Pursuant to the CSA, federal agencies were responsible for protecting such "sensitive" information and for developing plans to secure it "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."[37] The CSA, among other things, required agencies to develop security plans for systems containing sensitive information. It authorized the National Bureau of Standards (NBS), now called the National Institute of Standards and Technology (NIST), to create a security-oriented standards program. The definition of "sensitive information" was placed within the section that listed NBS's functions, and subsequently NIST became responsible when the agency's name was changed in 1988. In 1992, NIST issued guidance giving agencies authority to implement risk-based procedures to protect sensitive information pursuant to P.L. 100-235. NIST reiterated that "[i]nterpretation of the CSA's definition of sensitive is, ultimately, an agency responsibility." It identified three security goals:

> 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)."[38][Emphasis added.]

Although it was not mandatory, NIST urged agency information owners to use a risk-based approach to identify information to be protected and controls needed based on risk of loss:

> 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,

---

[37] 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.

[38] National Institute of Standards and Technology, "Advising Users on Computer System Technology," *CSL Bulletin*, Nov. 1992 [http://nsi.org/Library/Compsec/sensitiv.txt].

misuse, or unauthorized access to or modification of the information contained in the system.[39]

SBU in Relation to the Freedom of Information Act

Predating the CSA, 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,
(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.[40]

The CSA,[41] the report accompanying it,[42] and NIST guidance[43] included explicit instructions that categorizing information as "sensitive" did not confer authority to withhold information sought pursuant to Section 552 of Title 5, United States Code [the Freedom of Information Act]. Nevertheless, as will be discussed below, some federal agencies say that all information categorized as For Official Use Only (FOUO) or in related categories is SBU, or that all SBU information may be withheld under FOIA.

---

[39] "Advising Users on Computer System Technology," Nov. 1992, op. cit.

[40] 5 U.S.C. 552.

[41] According to P.L. 100-235, "Sec. 8. ... 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."

[42] 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" (House Report 100-153, Part I, June 11, 1987).

[43] 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" ("Advising Users on Computer System Technology," op. cit.)

Department of Justice Broadens Interpretation of Exemptions From FOIA in 2003 and 2004.[44] After the terrorist attacks of September 2001, the White House and the Department of Justice, in a series of administrative actions, expanded agencies' ability to withhold SBU information. To prevent potential use of sensitive information by terrorists, in March 2002, the White House issued the so-called "Card memo," which required agencies to examine their information holdings and policies; withhold information, including "sensitive but unclassified" information; and use FOIA exemptions if there was a sound legal basis to do so. Attorney General John Ashcroft's prior memorandum of October 2001 on this issue was referenced. These statements modified the previous Administration's policy, which urged agencies to release information if there was no "foreseeable harm" in doing so.[45]

---

[44] For detailed information, see CRS Report RL31845, op. cit.

[45] The White House 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," Mar. 19, 2002, required agencies to examine their policies and holdings in accord with 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). The purpose was to determine if information should be classified or handled as sensitive but unclassified information that could be "misused to harm the security of our Nation and the safety of our people" and report their review to the White House. The accompanying memo included a section titled "sensitive but unclassified information,"which instructed agencies to consider all applicable FOIA exemptions before releasing "sensitive information related to America's homeland security"(SHSI) ("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, "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security," Mar. 19, 2002). Agencies were referred to guidance that had been issued by Attorney General Ashcroft in Oct. 2001 that instructed agencies, when undertaking discretionary disclosure determinations under FOIA (agencies can make their own discretionary decisions about whether to disclose information even if it falls within one of the nine FOIA exemption categories) to consider using broad interpretations of the FOIA exemptions because of the need for heightened security in the wake of the 9/11 attacks ("New Attorney General FOIA Memorandum Issued," *FOIA Post,* Oct. 15, 2001, including "Memorandum for Heads of all Federal Departments and Agencies, From: John Ashcroft, Attorney General, Subject: The Freedom of Information Act, Oct. 15, 2001"). The memo instructed agencies to interpret FOIA exemption two broadly to permit withholding of a document that if released would allow circumvention of an agency rule, policy or statute, thereby impeding the agency in the conduct of its mission. (See U.S. Department of Justice, *Freedom of Information Act Guide and Privacy Act Overview*, May 2002, ed., pp. 16-17, 124-127 and CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security,* by John D. Moteff and Gina Marie Stevens.) 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.

In 2002 and 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. The

(continued...)

Subsequently in 2003, the Department of Justice (DOJ) issued guidance based on court decisions that broadened interpretation of exemptions from disclosure under FOIA.[46] It also discussed the new exemption three provision of P.L. 107-296, the Homeland Security Act of 2002, which protects voluntarily submitted critical infrastructure information. The *Freedom of Information Act Guide, 2004*, explained how an agency's ability to restrict the release of "sensitive" information via FOIA would be broadened; and, citing the September 11, 2001, attacks, the passage of P.L. 107-296, and the creation of the Department of Homeland Security (DHS), cautioned vigilance on releasing "sensitive" information:

> These changes have greatly impacted many aspects of the operation of the federal government, including the administration of the FOIA. Much greater emphasis is now placed on the protection of information that could expose the nation's critical infrastructure, military, government, and citizenry to an increased risk of attack. As a result of these changes, federal departments and agencies should carefully consider the sensitivity of any information the disclosure of which could reasonably be expected to cause national security harm.[47]

The *Guide* reiterated, however, that use of labels such as SBU. SHSI, and so forth does not "provide for any protection from disclosure under any [FOIA] exemption ..." [except for critical infrastructure information (CII), which is protected by statute]. Nevertheless, the *Guide* encouraged agencies to exempt from disclosure information labeled "SHSI" or other nonclassified information that is highly sensitive, as referenced in the aforementioned court decisions and in Homeland Security Presidential Directive HSPD-7, issued on December 22, 2003:

> [W]hatever the safeguarding label that an agency might (or might not) use for the information maintained by it that has special sensitivity — e.g., "for official use only" (FOUO), "restricted data" (a Department of Energy designation), or

---

[45] (...continued)
committee 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 (*A Citizen's Guide on Using the 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; and in a report with the same title, 108th Congress, 1st sess., 2003, H.Rept. 108-172).

[46] On June 25, 2003 officials from the DOJ's Office of Information and Privacy and from the National Security Council held a closed conference that was summarized on the DOJ website. (U.S. Department of Justice,"FOIA Officers Conference Held on Homeland Security," *FOIA Post*, July 3, 2003 [http://www.usdoj.gov/oip/foiapost/2003foiapost25.htm]). Among other things, it reviewed several court cases in 2003 that allowed agencies to use national security considerations, other than those defined in FOIA exemption 1, to withhold information of possible use to terrorists. These included one that allowed the U.S. Customs Service to use exemption 2 to deny information on inspections of seaport operations (*Coastal Delivery Corp. v. U.S. Customs Service*, decided Mar.17, 2003, by the U.S. District Court in Los Angeles), and another to allow withholding under exemption 7 (e) of "inundation maps"that had been compiled as law enforcement records and showed flood area below Hoover and Glen Canyon dams (*Living Rivers, Inc., v. the U.S. Bureau of Reclamation*, Mar. 25, 2003. by the U.S. District Court in Salt Lake City).

[47] *FOIA Guide, 2004 Edition*, Exemption one, [http://www.usdoj.gov/oip/foi-act.htm].

> "sensitive homeland security information" (SHSI) — whenever predominantly internal agency records may reveal information the disclosure of which could reasonably be expected to cause any of the harms described above [to critical systems, facilities, stockpiles, and other assets], responsible federal officials should carefully consider the propriety of protecting such information under Exemption 2.[48]

SBU Information Policies in the Homeland Security Act, P.L. 107-296, and Subsequent Presidential Action

The Homeland Security Act, P.L. 107-296, signed on November 25, 2002, defined homeland security information 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 to prevent, interdict, or disrupt terrorist activity; (C) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (D) would improve the response to a terrorist act."[49] The law, among other things, required agencies to develop information-sharing systems to transmit classified or unclassified information and to share it with appropriate recipients, including those at the state and local levels. It also recognized the use of nondisclosure agreements for sharing sensitive but unclassified information with state and local personnel. Section 892, as amended,[50] required the President to "prescribe and implement procedures" for federal agencies to "identify and safeguard sensitive homeland security information that is sensitive but unclassified," [now abbreviated SHSI] and to prescribe procedures to share this information with other federal agencies and appropriate state and local personnel (required by section 892 (a) (1) (A)(B) of P.L. 107-296). In Executive Order 13311, July 29, 2003, the President transferred some of these functions to the Department of Homeland Security Secretary, to be carried out in consultation with other governmental officials.[51] The President is still mandated to prescribe procedures for federal agencies. Section 893 of the law had required the President to report to specified congressional committees about implementation of section 892 and any recommendations for additional measures to "increase the effectiveness of sharing of information between and among Federal, State, and local entities." According to that report[52] and other documents,[53] in 2004,

---

[48] *FOIA Guide, 2004 Edition,* Exemption Two.

[49] 6 U.S.C. 482 (f).

[50] Amended by Section 316 of the Intelligence Authorization Act for Fiscal Year 2004, P.L. 108-177, Section 316, 117 Stat. 2599, 2610-11 (2003). This section mandates that DHS develop a training program for state and local officials to, among other things, improve their ability to identify and report threat information.

[51] Executive Order 13311, *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...."

[52] *Report Pursuant to Section 893,* not dated but reportedly sent to the committee chairmen in February 2004, op. cit.

[53] U.S. Department of Justice," FOIA Officers Conference Held on Homeland Security," *FOIA Post,* July 3, 2003, [http://www.usdoj.gov/oip/foiapost/2003foiapost25.htm].

DHS was preparing the guidance to identify and protect sensitive but unclassified SHSI. In its report to Congress, DHS wrote that the procedures it was developing

> will provide guidance on identifying SHSI by defining SHSI, establishing uniform procedures for identifying and marking SHSI, and delineating entities with which it may be properly shared. The procedures will aid in safeguarding SHSI by establishing uniform minimum standards for the secure handling of sensitive information designated as SHSI, in a manner consistent with existing law. Lastly, the procedures will help to facilitate the sharing of SHSI with appropriate Federal, state and local users, while also protecting it from unwarranted public disclosure that could result in reduction of the ability of Federal, State, and local authorities to protect against threats to our homeland security.[54]

The referenced guidance had not been issued as of February 15, 2006, but reportedly will be sent to the Office of Management and Budget for release and a period of public comment.[55]

In a related development, on December 16, 2005, the President issued a memorandum to federal agencies, "Guidelines and Requirements in Support of the Information Sharing Environment," that included requiring agencies to standardize procedures "for designating, marking, and handling SBU information ... across the Federal Government" in order to promote both appropriate, consistent safeguarding and sharing of information.[56] Within 90 days, agencies were to inventory their SBU information procedures, determine the authority for each entry, assess the effectiveness of procedures, and report to the Director of National Intelligence (DNI), who shall provide the results to the Secretary of Homeland Security and the Attorney General. Within a year, recommendations are to be submitted to the President through the DNI and other officials for government-wide standards for SBU information.

Requirements To Use Mandatory Minimum NIST-Generated Risk Standards To Protect All Information

As noted above, the Computer Security Act of 1987 (CSA) authorized the Department of Commerce's NBS (and then its successor, NIST) to develop standards and guidelines for federal agencies to protect sensitive information on federal computer information systems. The act defined sensitive information that was not classified. (For a definition, see the section above entitled "Computer Security Act Definition of Sensitive.") Under the CSA, agencies could obtain a waiver not to use the standards.

---

[54] *Report Pursuant to Section 893*, 2004, op. cit., p. 5.

[55] Interview with OMB officials, Nov. 10, 2004.

[56] Guideline 3. See memo at [http://www.fas.org/sgp/news/2005/12/wh121605-memo.html].

The CSA provisions were modified with passage of the Federal Information Security Act of 2002, (FISMA), P.L. 107-347, December 2002.[57] While CSA required the development of standards to protect sensitive information, FISMA required the development of standards to protect all information, and did not refer to sensitive information when mandating development of standards. It rewrote the section of the NIST act that required development of standards for sensitive information, and had used the CSA definition of "sensitive" information (15 U.S.C. 278g-3). The law replaced aspects of the CSA, including the definition of "sensitive" information because the definition was considered static and unresponsive to changing information systems environments.[58] FISMA also deleted specific requirements to inventory information systems that contained sensitive information.[59] These actions, in essence, rendered the definition moot. Also, under FISMA, agencies may no longer obtain a waiver to not use the standards developed by NIST.

Specifically, section 303 of P.L. 107-347 updated NIST's mission in light of new understandings relating to information security and required NIST, in consultation with other agencies, including OMB, the National Security Agency, the Government Accountability Office (GAO), and the DHS, to develop risk-based standards to categorize "the criticality and sensitivity of agency information according to information security control objectives and across a range of risk levels" and to develop minimum information security requirements for each information category. Under FISMA, the standards NIST was directed to develop and the Secretary of Commerce to promulgate, will be issued by the Director of OMB in

---

[57] FISMA clarified and changed some provisions of the Government Information Security Reform Act (GISRA), which was part of the Floyd D. Spence National Defense Authorization Act of FY2001 (Div. A, Title X, Subtitle G, sec. 1061-1065, P.L. 106-398, Oct. 30, 2000). While GISRA expanded NIST's functions regarding developing risk-based standards, it would have sunseted in 2002 and did not, like FISMA, render moot the definition of sensitive as used in CSA. See U.S. Congress, House, Committee on Government Reform, *E-Government Act of 2002*. House Report 107-787, Part 1, 107th Congress, 2nd sess., Nov. 14, 2002, pp. 54-61. Specifically, according to the report, "the purpose of FISMA is to permanently authorize a government-wide risk-based approach to information security by eliminating GISRA's two-year sunset, and to further strengthen Federal information security by requiring compliance with minimum mandatory management controls for securing information and information systems, clarifying and strengthening current management and reporting requirements, and strengthening the role of National Institute of Standards and Technology (NIST)" (p. 54).

[58] This was described in the House Committee on Government Reform report on the amended version of the bill that was enacted, House Report 107-787, part I, op. cit., describing section 303 of what eventually became P.L. 107-347.

[59] Section 305 of P.L. 107-347 repealed section 6 of the CSA, which required the identification of systems containing sensitive information and the development of systems security plans, which, according to the legislative report accompanying the bill that was enacted, "is unnecessary given the overall scheme and specific requirements for agency risk-based management of information and information systems supporting agency operations and assets" (House Report 107-787, pt. 1. p. 87. See also CRS Report RL31057, *A Primer on E-Government; Sectors, Stages, Opportunities, and Challenges of Online Governance*, Jeffrey W. Seifert).

consultation with the Secretary of Homeland Security.[60] They are to be mandatory minimum federal information processing standards (FIPS) that agencies and their contractors must use to protect all nonclassified information and information systems based on a range of risk levels.[61] FISMA is silent on defining "sensitive" or the relationship between the act and SBU or the sensitive homeland security information referred to in section 892 of the Homeland Security Act of 2002, P.L. 107-296.

FISMA also clarified management and reporting, strengthened NIST's role and responsibilities, and consolidated statutory information security requirements. The OMB is required by FISMA to authorize formally and accredit each agency's nonsecurity information system as established by the information security plan. (Responsibility for certification of national security information systems is shared between DOD and the Central Intelligence Agency.) The three security objectives — confidentiality, integrity, and availability — that NIST has used in previous guidance are to continue to guide NIST in its development of standards (116 STAT. 2947, P.L. 107-347, title III, paragraph 301), although these concepts were broadened from the way NIST originally used them in 1992 to read:

> The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide — (A) integrity, which means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information (Sec. 301 of P.L. 107-347).

The law also allows agencies to develop more stringent standards than those generated by NIST, since it —

---

[60] OMB, in consultation with the Secretary of Homeland Security, has responsibility under FISMA to issue the standards and guidelines developed by NIST (40 U.S.C. 11331 (b) (1) (A) and promulgated by the Secretary of Commerce. In addition, OMB manages the federal acquisition regulation (FAR). It is to be updated to include the information security requirements of FISMA, so that new agency contracts for information systems would reflect them. (U.S. GAO, *Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk*, April 2005, GAO-05-362.p. 3.) It appears that OMB has not yet issued the guidance. See also, U.S. GAO, *Information Security: Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements*, July 2005, GAO-05-552.

[61] Specifically, Title III of FISMA requires, "(b) Minimum requirements for standards and guidelines. The standards and guidelines required by subsection (a) of this section shall include, at a minimum — (1) (A) standards to be used by all agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels; (B) guidelines recommending the types of information and information systems to be included in each such category; and (C) minimum information security requirements for information and information systems in each such category ...." (U.S. Code, Title 15, Chapter 7, Section 278g- 3. Computer standards program, i.e., 15 U.S.C. 278g-3).

preserves the provision in current law (at 40 U.S.C 11331(c) permitting agencies to use more stringent standards than provided by NIST-developed standards, but only if those more stringent standards incorporate applicable mandatory NIST requirements and are otherwise consistent with the risk management policies and guidelines issued by OMB under 44 U.S.C. 3533.[62]

NIST's Policies, Standards, and Documents

The risk analysis procedures and information systems controls specified by NIST have been developed iteratively, incorporating public comments since the end of 2002, and implementation was to be mandatory (with NIST originally anticipating publication of all documentation by the statutory deadline of December 2005, a deadline which, it appears, was missed since publication has been delayed a few months).[63] Agencies are to use NIST's guidance documents and risk management procedures to categorize federal information and information systems and to determine security protection levels for them based on level of risk.[64]

Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal information and Information Systems, commonly called FIPS 199, issued in final form in February 2004, provides a common framework, method, and mandatory standards for agencies to use to identify information to protect (that is not governed by national security controls) according to the potential impact of loss. FIPS 199 enables "... agencies to identify and prioritize their most important information and information systems by defining the maximum impact a break in confidentiality, integrity, or availability would have on the agency's operation, assets, and/or individuals."[65] It establishes a continuum of "criticality and sensitivity" for information dependent upon agency requirements and priorities. The potential minimum impact value (low, moderate, or high[66]) on the compromise of a security objective is the highest value (i.e., high-water mark) for security categories for each type of information on the system.[67]

---

[62] Paragraph (a) (3) of section 302, according to House Report 107-787, pt. 1, p. 84.

[63] William Jackson, "FISMA Guidance Nearly Complete," *Government Computer News,* Oct. 26, 2005.

[64] Based in part on Ron Ross, "FISMA Implementation Project; Protecting the Nation's Critical Information Infrastructure; An Overview," Slide Show, Version 1.4.

[65] Shirley Radack, *ITL Bulletin,* Mar. 2004, p. 1.

[66] "... [L]ow [or limited], moderate [having a serious adverse effect], or high [severe or catastrophic adverse] impact for the three security objectives of confidentiality, integrity (including authenticity and non-repudiation), and availability"(Ron S. Ross, Computer Security Division, NIST, "The New FISMA Standards and Guidelines. Changing the Dynamic of Information Security for the Federal Government," [2003], p. 2. For additional details, see NIST, *Standards for Security Categorization of Federal Information and Information Systems,* FIPS Publication 199, Dec. 2003, pp. 1-3).

[67] As an example "... A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine

(continued...)

NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems,* issued in final version in June 2004,[68] is intended to help agencies identify their information types and systems and to assign *impact* levels for confidentiality, integrity, and availability for them for a range of risk levels. The impact levels are based on the security categorization guidelines in FIPS Publication 199.[69] Special Publication 800-60 gives agencies explicit guidance on developing impact standards for each of the three risk categories for all types of information and information systems handled by federal agencies (based on OMB's Federal Enterprise Architecture Program Management Office's publication, *The Business Reference Model Version 2.0*). Agencies are given guidance to determine impact levels for information in fields such as public health, environmental management, energy, and general sciences and innovation, including research and development. Thus the high-water mark, or highest value category for security impact (and thus minimum security categorization) for both "Scientific and Technical Research and Innovation Information" and for "Research and Development Information," is moderate.[70] Examples of minimum security categories for some other types of information are environmental remediation information, moderate;[71] pollution

---

[67] (...continued)
administrative information. The management at the power plant determines that (I) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as: SC sensor data = {(confidentiality, NA),(integrity, HIGH), (availability, HIGH)}, and SC administrative information = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}. The resulting security category of the information system is initially expressed as: SC SCADA system = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)}, representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as: SC SCADA system = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}." (FIPS 199.)

[68] William C. Barker, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST Special Publication 800-60, Version 2.0, June 2004, pp. 21-22. William C. Barker and Annabelle Lee, NIST, *Information Security, Volume II: Appendixes to Guide for Mapping Types of information and Information Systems to Security Categories,* June 2004, 295 pages.

[69] Barker, *Volume 1,* NIST Special Publication 800-60, June 2004, op. cit., pp. 21-22.

[70] NIST Special Publication 800-60, op. cit., pp. 217-218.

[71] NIST Special Publication 800-60, op. cit., pp. 154-155.

prevention and control, low;[72] and health care services, high.[73] Each explanation describes circumstances, including homeland security and national security-related implications, that agencies could identify to raise the threshold level of security controls for each type of information.

NIST's publication *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, September 2004 and February 2005, provides interim guidance for minimum security control procedures for low, moderate, and high impact information systems until completion and adoption of the anticipated *Minimum Security Controls for Federal Information Systems*, Federal Information Processing Standards (FIPS) Publication 200, which may be published in early 2006.[74] When agencies need to evaluate the levels of protection for information, they are to undertake a risk assessment using threat and vulnerability analysis that incorporates local conditions and then adjust their security controls using NIST publication SP 800-30.[75] After determining the security category, an agency identifies the minimum information security requirements (i.e., management, operational, and technical controls) for information and information systems in each such category as identified in document 800-53. NIST identified 17 types of security control clusters to guide selection of minimum security controls (i.e., safeguards and countermeasures) to protect information and information systems and 154 uniquely identified controls (i.e., management, operational, and technical security controls) for information and information systems in each category. These include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.[76] The controls an agency selects to protect information depend upon analysis of threat, vulnerabilities, and impacts.

A Formal Risk Analysis Process Is Not Required. OMB's apparent operative guidance for information security protection, Appendix III of OMB Circular A-130,[77] cautions agencies that they do not need to conduct expensive,

---

[72] NIST Special Publication 800-60, op. cit., p. 120.

[73] NIST Special Publication 800-60, op. cit., p. 120.

[74] Jackson, Oct. 26, 2005, op. cit. As of February 15, 2006, the document is finished but is awaiting approval by the Secretary of Commerce. (See [http://csrc.nist.gov/sec-cert/milestone-schedule-v23.pdf].

[75] *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*, by Gary Stoneburner, Alice Goguen, and Alexis Feringa, NIST, SP 800-30, July 2002.

[76] NIST, *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, Appendix D and Appendix F.

[77] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," to "OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources (11/28/2000)," requires agencies and their contractors to (continued...)

formal risk analyses to fulfill these requirements. Specifically, Appendix III to OMB Circular A-130 says that OMB

> no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995).[78]

While NIST recognizes this dictum, it seems that little information is available about how agencies make decisions to categorize information in response to NIST standards.[79]

Nongovernmental Experts' Recommendations to Use Risk Analysis To Identify and Control Sensitive Information

Nongovernmental experts have recommended using various types of risk-based processes to identify, categorize, and develop controls for sensitive information involving science and technology, and other kinds of information control.[80] For instance, the use of risk analysis figured prominently at the November 21, 2005 meeting of the National Science Advisory Board for Biosecurity (NSABB) in discussions related to developing criteria for a code of conduct for researchers, identification of code violations, and development of appropriate consequences. Risk

---

[77] (...continued)
maintain programs that provide adequate security for all information collected, processed, transmitted, stored, or disseminated in general support systems and major applications" ([http://www.whitehouse.gov/OMB/circulars/a130/a130appendix_iii.html]).

[78] Appendix III, to OMB Circular A-130, 11/28/2000, op.cit.

[79] Interviews with officials at NIST and GAO.

[80] *Horizontal Integration: Broader Access Models for Realizing Information Dominance* is a report prepared by the Defense Department JASON advisory group for the Under Secretary for Defense Research and Engineering, *Horizontal Integration: Broader Access Models for Realizing Information Dominance*, JASON Program Office, MITRE, JSR-04-132, Dec. 2004, p. 1. The report focused on the goal of enabling "information dominance [in] warfare" and concluded that more information should flow directly to military personnel in the field, who might not always have clearance levels required to handle classified information or sensitive information, which is "....increasingly defined by the eye of the beholder"(pp. 4, 24-30). The report recommended using an information system based on "... transactional risk — that is the chance that any given transaction will be compromised, rather than on assigning a level of classification to a document based on the potential damage caused by disclosure" (Shaun Waterman, "Report: Govt Secrecy Hurting War Fighters," *UPI*, Dec. 15, 2004).

analysis has also figured in NSABB discussions about developing a process and time schedule to vet and communicate dual-use research while it is being conducted and before publication, and about determining the consequences of public release.[81] (For more information about NSABB, see in the section below entitled "National Science Advisory Board for Biosecurity.") Others have also proposed using risk-based models to handle sensitive scientific and technical information. These are discussed next.

Jacques S. Gansler and William Lucyshyn proposed that criteria be developed, and that an executive order be issued, that identifies "controlled unclassified security information (CUSI)," consisting of CII and SHSI, whose improper release by government or academic/scientific institutions "... could egregiously endanger public safety."[82] The objective "... for both government-funded and privately-funded research is to create a culture that frowns on the research, experimentation, and publication of CUSI, much like the culture that constrains certain experimental techniques, such as stem-cell research, and restrains others, such as human cloning."[83] A risk-based process called a "'Work-Factor' for Leveraging Dangerous Information" — the amount of resources needed to use the information for harmful purposes — would be used to determine risk of release:

> When information that could threaten the public safety is easily accessible — that is, when the costs of obtaining it are low and the convenience of using it is relatively high — this "work-factor" for leveraging potentially harmful information provides a benchmark for determining whether information should be controlled. While high-level descriptions of and mitigations for vulnerabilities should be released to inform and alert the public, "push-button" or "cookbook" instructions on how to do harm are easily identifiable and clearly should be withheld. The amount of resources, including the number of knowledgeable personnel, needed to exploit vulnerabilities describes a work-factor, which is a good, practical indicator of where disclosure borders on weaponization.[84]

---

[81] The archived webcast of the Nov. 21, 2005 meeting is available at [http://videocast.nih.gov/ram/od112105.ram]. See also, Andrew J. Hawkins, "National Biosecurity Panel Lays Groundwork for Identifying Dual-Use Research," *Research Policy Alert*, Nov.22, 2005; Andrew J. Hawkins, "Success of Scientist Code of Conduct Hinges On Education, Biosecurity Board Hears," *Research Policy Alert*, Nov.23, 2005; and Eugene Russo, "Biosecurity Advisory Board Reports Lessons Learned From 1918 Flu Papers, Aims to Improve Screening Process," *Research Policy Alert*, Nov. 23, 2005.

[82] Jacques S. Gansler and William Lucyshyn, *The Unintended Audience: Balancing Openness and Secrecy: Crafting an Information Policy for the 21st Century*, Center for Public Policy an private Enterprise School of Public Policy, University of Maryland, Sept. 2004, pp. 27, 32.

[83] *The Unintended Audience: Balancing Openness and Secrecy*, op. cit., pp. 38-39.

[84] *The Unintended Audience: Balancing Openness and Secrecy*, op. cit., pp. 40-42. The following illustrations were given "[f]or potential low-impact events, the most serious threats are those that are highly convenient and extremely low cost.... Typically, these threats cause a high level of disruption and/or annoyance. An example of such a threat would be contaminating food with bacteria, similar to the 1984 case where members of a religious cult sprayed salmonella bacteria on salad bars throughout the Oregon region, (continued...)

The report recommended that with respect to "public sector information," a policy embodying CUSI would "enable the sharing of sensitive materials between departments and agencies at the federal, state, and local levels, as well as with those in the private sector with a need to know,"[85] and would ensure "... that similar information produced in different agencies is identified and protected in the same way" and that FOIA and CUSI guidelines are not in conflict."[86] DHS, it was recommended, should develop educational programs, government controls, and voluntary restraints to prevent the disclosure of information that should not be released.[87] Government-defined policy controls should extend to publicly funded private researchers and DHS, assisted by NSF and NIH and other agencies, should issue guidance to privately funded researchers. Professional peer reviews would be conducted before publication of work that might meet criteria for safeguarding. Specifically,[88]

> [f]ederally-funded researchers should disclose potential security concerns in their grant proposals. DHS monitored review panels will assess the security implications of the work with potentially significant negative impact in accordance with established guidelines. DHS should lead the effort to develop model review policies, encouraging non-federally-funded researchers to adopt them and to submit their work to the government-monitored review panel or an independent, government-certified review panel. DHS should also train publishers to conduct reviews just before research is made available to serve as a safety net after research is already completed, and publishers should implement a two-tiered publication scheme to restrict detailed content to premium access where the credentials of the readers can be verified.[89]

---

[84] (...continued)
causing 751 cases of food poisoning.... For a potential medium-impact event, those threats that are high in cost and low in convenience warrant the least amount of concern.... Information on agents that when directly applied to fields would decrease crop yield without completely destroying the harvest might fall into this category. It would be difficult to deliver such agents, and decreasing the yield for some crops in the United States might succeed only in reducing the surplus. Nearly all of the threats of a potential high-impact event should be considered serious, and information related to these threats should be controlled.... A grey area, where information would have to be carefully evaluated, forms when costs are high and convenience is low. For example, information on how to create vaccines for highly-communicable diseases could fall into this category, as the method for creating vaccines now in use first increases the virulence of normal diseases and then finds inhibitors to block or antibodies to combat the strongest variants of the diseases. Increasing controls significantly could slow the development of preventive measures, which, in the end, might cause more harm than good" (*The Unintended Audience: Balancing Openness and Secrecy,* op. cit., pp. 43-44).

[85] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit.,p. ii, p. 33.

[86] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit., p. 33.

[87] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit., p. 44.

[88] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit., p. 45.

[89] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit., pp. ii-iii.

Brian J. Gorman proposed a risk-based alternative approach for prepublication peer review. He called for a risk-based process called "Due Process Vetting System" (DPVS) together with "... a Risk Assessment Scale [RAS] and a Least Restrictive Classification System for the communication, assessment, and disposition of sensitive life science research in a manner consistent with national security interests."[90] The aforementioned reports proposed that researchers should self-evaluate the sensitivity of their work and that self-imposed professional association or governmental constraints, including classification, be imposed if the information could be weaponized and if the consequences of its use were high risk, but that such information should be communicated among those with a "need to know."[91] (This proposal and others for institutional or governmental bodies to review and approve biological sciences research plans or publications are discussed below in the section "Controls on Unclassified Biological Research Information.")

Policies To Protect Specific Types of Sensitive Information Involving Scientific and Technical Applications

Specific laws have been enacted and policies and procedures are in varying stages of implementation that define and protect sensitive unclassified science- and technology-related information in such fields as critical infrastructure, transportation, environmental impacts, biology, geospatial data, and DHS information. These and criticisms that have been made about them are summarized next.

Critical Infrastructure Information Controls

The need to protect critical infrastructure information is based on the premise that potential terrorists should not have access to information that might expose vulnerabilities in, or provide roadmaps to, the nation's core physical transportation,

---

[90] Brian J. Gorman, "Balancing National Security and Open Science: A Proposal for Due Process Vetting," *Yale Journal of Law and Technology*, 2005, pp. 2, 15.

[91] *The Unintended Audience: Balancing Openness and Secrecy*, op. cit., pp. 39-40. See also J. Gaudioso and R. M. "A Conceptual Framework for Biosecurity Levels," *BTR 2004: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism — Proceedings*, Albuquerque, NM, March 18-19, 2004, p. ii. As an illustration: "Restricting research and development must rely on constraining knowledge rather than forbidding it. For example, such restrictions would control research into the engineering of viral factors that introduce animal pathogens into humans but would not prohibit it, categorically. Production refers to the ways in which information can be weaponized, or leveraged against the public. As such, production restraints should entail issues similar to ways of refining anthrax and ways of enriching uranium. Although information about weapons programs would be classified, scientific "know-how" that may be — as in the case of bioweapons — only one step away from implementation generally would not be classified. Employment refers to final-stage delivery. For example, issues of employment may refer to detailed schematics on the briefcases used in the Tokyo sarin gas attacks or plans for maximizing the radiological contamination from a "dirty bomb" (Gaudioso and Salerno, op. cit., Mar. 18-19, 2004, p. 28).

water, communication, energy, and related systems, or to major buildings, bridges, and other types of major structures. As an example of critical infrastructure vulnerabilities, Charlie Reeder, Interagency Operations Security Support Staff, DOD, and part of a Pentagon group that represents the National Security Agency, Central Intelligence Agency, Federal Bureau of Investigation, DOD, General Services Administration, and Department of Energy (DOE), is reported to have said that "'... he's seen government Web sites include maps of installations ... specifications of weapons and communications systems ... and much more. ... When we publish this information on the Internet, we might as well fax it directly to our adversaries ...'"[92] He also commented that "'According to a message sent by Secretary of Defense Donald Rumsfeld ... an al Qaeda training manual recovered in Afghanistan states 'using public sources openly and without resorting to illegal means, it is possible to gather at least 80 percent of information about the enemy.'" Open-source information can be accessed through Internet sites, job announcements, budget documents, and newsletters.[93] Similarly, a survey by *Computerworld* noted that "the widespread availability of sensitive information on corporate websites appears to have been largely overlooked by IT and security managers...."[94] Among the information available on the Web are "3-D models of the exterior and limited portions of the interior of the Citigroup headquarters building in Manhattan — one of the sites especially named in the latest terror advisory issued by the Department of Homeland Security," and various similar kinds of information about the building's structural design weaknesses.

In part to cope with issues like these, the "Critical Infrastructure Information Act of 2002," Title II of P.L. 107-296, prohibits disclosure under FOIA of "critical infrastructure information" (CII) relating to the security of critical infrastructure and protected systems submitted to DHS voluntarily by private companies.[95] Criminal penalties for disclosure by employees under this statute include fines, dismissal, or imprisonment for up to a year (Section 214).[96] The statute also provides 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.[97] The DOD issued a memo on March 25, 2003, that applied prohibitions like those in P.L. 107-296 to critical infrastructure information

---

[92] Stephen Larsen, "Secure Sensitive Unclassified Information," *Pentagram*, Nov. 28, 2003 [http://www.dcmilitary.com/army/pentagram/8_47/commentary/26442-1.html]).

[93] Larsen, op. cit.

[94] "Too Much Info on Websites," *SAP Info*, Sept. 8, 2004.

[95] Sections 211-215 of P.L. 107-296, codified as 6 U.S.C. 131-134, define the term "critical infrastructure information" to mean information not customarily in the public domain and related to the security of critical infrastructure or protected systems. For rules, see 6 C.F.R. 29.1 and 6 C.F.R. 29.2.

[96] For additional analysis, see CRS Report RL31547, op. cit.

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

voluntarily submitted to DOD.[98] On April 15, 2003, DHS published interim rules to implement the critical information infrastructure protection provisions of P.L. 107-296, which would extend the rules to other agencies by requiring them to pass to DHS similar information that they receive.[99] On December 17, 2003, President Bush issued Homeland Security Presidential Directive 7 (HSPD-7), which among other things, directed all federal agencies to protect voluntarily submitted information about critical infrastructure vulnerabilities in line with Title II of P.L. 107-296.

The DHS published an interim final rule that established the "Protected Infrastructure Information (PCII) Program," effective February 18, 2004, with public comments allowed until May 20, 2004.[100] It requires submitters 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. If agencies other than DHS obtain comparable information in their normal regulatory processes, the CII restrictions do not apply; if a company submitted information to DHS under the protected CII program that was identical to information required by another agency, the protection afforded to the submission to DHS would not extend to the information submitted to another agency. This latter provision is intended to allay some of the fears that 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.[101] CII information submitted to DHS is not subject to disclosure under FOIA, under a new exemption three category, pursuant to section 214 of the Homeland Security Act of 2002,[102] if it has not been made public previously.[103] The language in P.L. 107-296 protects

---

[98] 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.

[99] "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.

[100] The implementing regulations are contained in the *Code of Federal Regulations* (6 CFR Part 29). See also 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. Comments are posted on the DHS website. See also Lucy A. Dalglish and Gregg P. Leslie, *Homefront Confidential*: *How the War on Terrorism Affects Access to Information and the Public's Right to Know*, fifth ed., 2004, pp. 70-71.

[101] Dalglish and Leslie, op. cit., pp. 70-71.

[102] 6 U.S.C.A. section 133. See the memo on "Critical Infrastructure Information Regulations Issued by DHS," *FOIA Post*, Feb. 27, 2004, [http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm], Leslie, op. cit., and CRS Report RL30153, op. cit.

[103] DHS press release, Feb. 18, 2004, op. cit.

only CII submitted to the DHS, but the Department of Justice reports that in the future, it may be applied to submissions made to other federal agencies.[104]

Sensitive Security Information Controls: Transportation

The Federal Aviation Administration (FAA) had been permitted since passage of the Air Transportation Security Act of 1974[105] to issue regulations to protect, and to distribute to those with a "need to know," sensitive civil aviation security information that was obtained during security investigations or consisted of research and development information that would invade privacy, would reveal a trade secret or financial or commercial information, or would be detrimental to the safety of persons traveling by air. "The FAA implemented this authority by promulgating regulations, which, among other things, established a category of information known as Sensitive Security Information (SSI). In 1997, the Department of Transportation (DOT) definition of SSI included 'records and information ... obtained or developed during security activities or research and development activities.'"[106] Subsequently, this type of information was given a statutory basis pursuant to the Aviation and Transportation Security Act, P.L. 107-71, which created the Transportation Security Administration (TSA) and prohibited disclosure of certain kinds of information relating to transportation if the disclosure would be detrimental to the safety of passengers in transportation.[107] P.L. 107-296 expanded this coverage to include information detrimental to the "security of transportation." As the FAA was moved to the TSA, first located in the DOT and then to the DHS,[108] the SSI withholding authority appears to have been expanded to include "all transportation related activities including air and maritime cargo, trucking and freight transport, and pipelines."[109] On May 18, 2004, the DOT and DHS jointly promulgated revised regulations,[110] which, "adopt the Homeland Security Act language as the definition of SSI. In addition, the new regulations incorporate former SSI provisions, including

---

[104] "Critical Infrastructure Information Regulations Issued by DHS," op. cit. 2004.

[105] Air Transportation Security Act of 1974, P.L. 93-366, Section 316, 88 Stat. 409 (1974), as cited in CRS Report RL32664, *Interstate Travel: Constitutional Challenges to the Identification Requirement and Other Transportation Security Regulations*, by Todd B. Tatelman,

[106] According to Tatelman, op. cit., codified at 14 C.F.R. § 191.1 (1997).

[107] Created pursuant to the Aviation and Transportation Security Act (ATSA), P.L. 107-71, section 101 (e)(3), 115 Stat. 597, 603 (2002).

[108] For detailed history of the laws and regulations that govern SSI and transportation, see CRS Report RL32664, op. cit., and CRS Report RL32425, *Sensitive Security Information and Transportation Security: Issues and Congressional Options*,Mitchel A. Sollenberger.

[109] CRS Report RL32664, op. cit.

[110] See also "Protection of Sensitive Security Information, Transportation Security Administration (TSA), DHS, and Office of the Secretary of Transportation (OST), DOT." *Federal Register*, May 18, 2004 (v. 69, no. 96), pp. 28066-28086. (DOT, Office of the Secretary of Transportation, 49 CFR Part 15; Department of Homeland Security, Transportation Security Administration, 49 CFR Part 1520.)

the sixteen categories of information and records that constitute SSI."[111] SSI information is defined by statute (49 U.S.C. section 114 (s)) and an implementing regulation (49 C.F.R. part 1520)[112] as

> (1) Security programs and contingency plans ... issued, established, required, received, or approved by DOT or DHS.... (2) Security Directives.... (3) Information Circulars ... issued by DHS or DOT regarding a threat to aviation or maritime transportation.... (4) Performance specifications.... (5) Vulnerability assessments.... (6) Security inspection or investigative information.... (7) Threat information.... (8) Security measures.... (9) Security screening information.... (10) Security training materials.... (11) Identifying information of certain transportation security personnel.... (12) Critical aviation or maritime infrastructure asset information.... (13) Systems security information... (14) Confidential business information.... (15) ... Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS or DOT, including research results... (16) Other information....

This information, like CII information, was also designated as exempt from disclosure under FOIA (49 U.S.C sec 40119(b) (1)) under exemption 3, which permits the withholding of information protected by other statutes, has use limitations for sharing with state or local governments, and imposes criminal penalties on federal officers or employees who disclose such information.[113]

Critique of SSI Rules. The ability of terrorists to capitalize on vulnerabilities in the national and foreign transportation systems in this arena have been manifested several times since 2001. Nevertheless, some critics charge that too much information is being withheld from public access. Many of the criticisms of SSI rules focus on the alleged consequences of preventing the public from accessing information that might be used to promote safety or be used in citizen oversight. For instance, some aircraft personnel and consumer advocates say that TSA's use of SSI can "muzzle debate of security initiatives and insulate TSA from criticism."[114] The newsletter *OMBWatch* reported that the TSA has denied access to information when "reasonable access to it could improve safety conditions for communities and workers."[115] Examples include TSA denying pilots access to information to comply

---

[111] Tatelman, op. cit., pp. 3-4. See the original for footnotes to this quotation.

[112] *Report Pursuant to Section 893*, not dated but reportedly sent to the committee chairmen in February 2004, p. 5, op. cit.

[113] See CRS Report RL32597, *Information Sharing for Homeland Security: A Brief Overview*, by Harold C. Relyea and Jeffrey W. Seifert.

[114] *Secrecy in the Bush Administration*, by U.S. House of Representatives, Committee on Government Reform — Minority Staff Special Investigations Division Prepared for Rep. Henry A. Waxman, Sept. 14, 2004, p. 54. Tim Starks, "A Fine Mess: TSA's New Information Security Rules Leaves Stakeholders Confused," *CQ Homeland Security*, July 21, 2004.

[115] "Transportation Agency Hides Vital Data 'Sensitive Security Information,'" *OMB Watch*, (continued...)

with TSA regulations to avoid flying near nuclear power plants, disagreeing with TSA's views that information on such sites compiled from public data by the Aircraft Owners and Pilots Association should be labeled SSI and not be made available, and denying the District of Columbia government access to information to help them determine if trains carrying chlorine through D.C. should be rerouted. The Coalition of Journalists for Open Government (CJOG), a group of journalist advocacy organizations,[116] in a filing on July 16, 2004, in response to regulations jointly filed by the Department of Transportation and the Transportation Security Administration,[117] said

> [The] ... unrestricted use of the ... (SSI) designation ... will have a seriously adverse impact on traditional citizen and media oversight of the governance of our seaports, airports and transit systems.... There appear to be no limits to the type of information that might be gathered or generated as SSI and then sealed. Local and state officials, bound by non-disclosure agreements, may be forced to deny access to records that state law and local ordinance require be made available to citizens. Information needed by civic activists or organizations to maintain oversight and challenge local officials on their management of public facilities may be withheld, even when the information's relevance to any possible terrorist threat is at best tenuous. [118]

In the same document,[119] the CJOG recommended that federal agencies should preserve public access to what it calls "critical oversight information" (COI) — "any information a citizen might use to judge whether his or her public servants are serving well," information "that speaks to the quality and integrity of their performance as policy makers, managers or employees of our seaports, airports and transit systems," including budget information and details on revenue and spending and information about personnel and their qualifications, training, and performance.[120]

---

[115] (...continued)
Apr. 4, 2005.

[116] Composed of American Society of Newspaper Editors; Associated Press Managing Editors; Committee of Concerned Journalists; National Association of Science Writers; Newspaper Association of America; Reporters Committee for Freedom of the Press; Radio-Television News Directors Association; Society of Professional Journalists; Society of Environmental Journalists.

[117] See also "Press Coalition Defends Access to "Critical Oversight Info," *Secrecy News,* July 19, 2004.

[118] Pete Weitzel, "Comments of the Coalition of Journalists for Open Government (CJOG), Before The Department of Transportation and the Transportation Security Administration, In the Matter of *Protection of Sensitive Security Information*," RIN 1652 AA08 Docket # TSA 2003-15569.

[119] These comments were made in a filing by CJOG and nine of its member organizations on July 16, 2004, in response to regulations jointly filed by the DOT and the TSA involving the designation and disclosure of information designated as Sensitive Security Information.

[120] Weitzel, CJOG, op. cit.

Controls on Environmental Impact Information

Controls on environmental impact information are premised on the need to protect internal agency decision making procedures and to control access to information that terrorists might use to harm critical infrastructures, deliver services, or poison the, air, water, and so forth. The actions discussed next represent steps that have been taken to safeguard public access to environmental information.

The Department of Homeland Security (DHS) expanded its ability to withhold certain types of environmental impact information that previously was available to the public pursuant to the National Environmental Policy Act (NEPA).[121] On June 14, 2004, DHS issued a directive proposing new categorical exclusions to disclosure requirements under FOIA for assessments of environmental impacts of DHS decision making and included component DHS agencies in the categorical exclusions policy.[122] The directive specified three levels for projects or grants that might have environmental impacts: "those affecting national security that are categorically excluded from coverage under NEPA; those that require DHS agencies to conduct environmental assessments; and those with the greatest potential to affect natural resources and the environment, which would require more detailed environmental impact statements." Specifically, EPA allows categorical exclusions for "actions that ... do not ... have significant impact on the human environment, and therefore ... do not require an environmental assessment ... or environmental impact statement...." (40 C.F.R. 1500-1508.)

Some of the agencies that were transferred to DHS had previously identified such exclusions. In addition, the directive exempted all DHS agencies (Transportation Security Administration, Coast Guard, Border Patrol, FEMA and others) from releasing classified, proprietary, or other information exempt from disclosure under FOIA, and proposed to exempt critical infrastructure information, sensitive security information, and other information described in "laws, regulations, or Executive Orders prohibiting or limiting the release of information."[123] Some say this could exclude from public view environmental impact statements required by NEPA. In its *Federal Register* announcement, DHS said that it would place protected information prepared for compliance with NEPA into appendix sections for viewing only by decision makers, but would allow the public to view nonsensitive portions of the material. However, it added "...if segregation would leave essentially meaningless material, the DHS elements will withhold the entire NEPA analysis from the public." The plan also would allow DHS to categorize some environmental reviews as "sensitive security information" or "critical infrastructure information" exempt from public disclosure. The public comment period was for one month and then was extended to August 16, 2004. DHS held a meeting on October 12, 2004 to

---

[121] 42 U.S.C. Section 5321 et. seq.

[122] DHS, "Proposed Management Directive 5100.1, Environmental Planning Program," *Federal Register*, v. 69, no. 33043- 33066. June 14, 2004.

[123] *Federal Register*, June 14, 2004, op. cit., p. 33063.

discuss public comments received.[124] No further publicly announced information appears to have been released about this policy.

A 2005 supplemental appropriations bill (H.R. 1268), enacted as P.L. 109-13,[125] exempted the DHS from certain legal requirements when physically securing U.S. borders. Some contend that this may enable DHS to waive environmental protection laws, among others, relating to border security.[126]

Critiques of Controls on Environmental Information. Some critics allege that these types of policies, including SBU information control policies, conflict with the environmental quality laws of the 1970s and the Emergency Planning and Community Right-To- Know Act of 1986 (42 U.S.C. 11049). Critics of regulations limiting access to some critical infrastructure information focus on their preemption of state and local disclosure laws and the inability of citizens to obtain information needed to ensure community safety.[127] Several environmental

---

[124] Management Draft Management Directive 5100.1, Environmental Planning Program Meeting Minutes, Subject: Draft Environmental Directive for the Department of Homeland Security (DHS) Meeting: October 12, 2004, at [http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0528.xml].

[125] According to Sec. 102 of P.L. 109-13: "Waiver of Legal Requirements Necessary for Improvement of Barriers at Borders; Federal Court Review," Section 102(c) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (8 U.S.C. 1103 note) is amended to read as follows: "... Notwithstanding any other provision of law, the Secretary of Homeland Security shall have the authority to waive all legal requirements ... [he] determines necessary to ensure expeditious construction of the barriers and roads under this section.... Any such decision by the Secretary shall be effective upon being published in the *Federal Register*."

[126] "Homeland Security Wins Power to Waive All Law," *OMB Watch*, Feb, 2005.

[127] Reportedly, once submitted to DHS, "information that is designated CII is not merely exempt from public disclosure. It can't be disclosed to any government official except for national security purposes. Nor can it be used in court. That means a company could tell the Department of Homeland Security about an eroding chemical storage tank on the bank of a river, but DHS could not disclose that information to the public or even to the Environmental Protection Agency. And if there were a spill ... , the information given DHS couldn't be subpoenaed in a law suit. No one knows just what that will mean in practice, but the concern is palpable" (Pete Weitzel, "A Skip Through the Rabbit Hole," *The American Editor [American Society of Newspaper Editors]*, May-June-July 2004).

Problems were reported by a community group working with the Project on Government Oversight (POGO) "to track drinking water supplies contaminated with perchlorate, a rocket fuel that causes developmental problems in children. After 9/11, the Army refused to share critical information with the community groups, including maps of drinking water test wells. What confused community groups the most was the fact that these maps were already shared publicly — but the Army refused to acknowledge them and claimed they were 'sensitive' information not for public release. The community group refused to back down and is now suing the Army for information under an environmental law that gives community groups the right to be informed about toxic chemical threats" ("Fighting Secrecy — And Winning," *OMB Watch*, Feb. 23, 2004. For additional examples of the issue of SBU in the environmental area, see, Richard Dahl, "Does Secrecy Equal Security?" *Environmental Health Perspectives*, Feb. 2004, pp. A104-A107). See also (continued...)

groups have criticized controls on environmental information, including the DHS environmental directive released on June 14, 2004. The Natural Resources Defense Council charged that because the agencies subsumed by DHS make environmentally related decisions relating to oil spills, border security, flood planning, and chemical plant security, and so forth, communities should be given an opportunity to evaluate these decisions.[128] In addition, some agencies label environmental impact statements as SBU, saying that they should be released only to those who have a "need to know." Some agencies post environmental impact materials on the Internet with blacked-out markings for what appears to be locational or infrastructure details.[129] Other agencies have published documents and put SBU information into a separate appendix, available under controlled access. Generally, because of "security sensitivity," most DOE environmental assessment documents are not available to the public online but may be accessible via hardcopy in NEPA reading rooms if the requestor qualifies.[130]

The American Library Association (ALA) proposed that, with respect to environmental information, DHS should limit "its non-disclosure provision to information that unambiguously qualifies for withholding under one of the exemptions provided in the Freedom of Information Act...."[131] It contended that the provision allowing DHS to withhold "essentially meaningless" information not now subject to exemption from disclosure should be deleted since Congress intended the public to determine what information is meaningful in the environmental statements. *OMB Watch* concurred: "There are no procedures contained in the directive for how DHS will determine which pieces of environmental analysis to remove if it falls within an exemption, or how it will determine if the public finds the information meaningful."[132]

---

[127] (...continued)
regarding withholding of flood inundation maps, Gregg Sangillo, "Groups Raise Concerns About Increased Classification of Documents," *GovExec.com,* Oct. 27, 2004.

[128] National Resources Defense Council, *Comments to Proposed Management Directive 5100.1, Environmental Planning Program,* July 14, 2004, as cited in *Secrecy in the Bush Administration,* op. cit., Sept. 14, 2004, p. 56. See also regarding access to maps locating perchlorate plumes, "Post 9-11 Secrecy Hits Homer in Aberdeen Maryland," Release prepared by the Working Group on Community Right-to-Know, Jan. 29, 2004.

[129] See, for instance, U.S. Department of Energy, *Environmental Assessment For the Strategic Petroleum Reserve West Hackberry Facility Raw Water Intake Pipeline Replacement Cameron and Calcasieu Parishes, Louisiana,* DOE/EA-1497 [http://www.eh.doe.gov/nepa/ea/EA1497/EA-1497.pdf] and "NRC Censors Environmental Impact Statement,"*OMB Watch,* Jan. 24, 2005.

[130] Source: [http://www.eh.doe.gov/nepa/documents.html].

[131] Emily Sheketoff, American Library Association, Letter "Re: Department of Homeland Security's Proposed Management Directive 5100.1, Environmental Planning Program," Aug. 16, 2004.

[132] "DHS Seeks Exemptions From Public Disclosure Requirements," *OMB Watcher,* July 29, 2004. See also,: Mike Ferullo, "Groups Wary of Homeland Security Plan Exemptions Some Environmental Reviews," *Daily Report for Executives,* July 16, 2004, p. A-21.

Illustration of Complexity of the Issue: the Nuclear Regulatory Commission (NRC). The complexity of balancing access to, and protection of, information is illustrated by actions taken by the Nuclear Regulatory Commission (NRC). In August 2004, the agency issued a statement that "certain security information formerly included in the Reactor Oversight Process will no longer be publicly available."[133] Its efforts to "scrub " its website while balancing public access and information security generated public criticism that NRC withheld information relevant to the safety of surrounding residents but shared such information with power companies and industrial lobbying groups. The NRC also allegedly threatened criminal prosecution for persons who published critiques of two nuclear reactors in Indian Point, New York, even though the NRC is reported to have said it could not specify what information was compromised.[134] In the fall 2004, some "... news and watchdog organizations pointed out that some sensitive documents in the [NRC online] library could be used by terrorists"; the NRC subsequently closed major portions of the library and reviewed items it contained.[135]

Representative Edward J. Markey, a senior minority member of the House Committee on Energy and Commerce, wrote to the NRC, requesting that its inspector general investigate the agency's information release policies and, specifically. concerns about the NRC "improperly restricting access to specific documents that should be releasable from a security perspective but are nevertheless being withheld from public release." [136] He cited the agency's proposals to widen its definition of "proprietary information" to withhold more public information and to broaden restrictions on the dissemination of sensitive information to include emergency evacuation plans and safety analyses concerning the protection of nuclear materials; its actions to withhold an unclassified version of an NAS report allegedly because the NRC disagreed with its findings; and the agencies' prohibitions on non-industry representatives attending meetings and having information, even though industrial representatives were given access. In June 2005, the Nuclear Regulatory Commission announced it would restore viewing on the web to more than 70,000 documents, after reviewing them for "sensitive security information."[137] An NRC

---

[133] "NRC Modifies Availability of Security Information From All Nuclear Plants" *NRC News,* Aug. 4, 2004 (No. 04-091).

[134] R. Jeffrey Smith, "Nuclear Security Decisions Are Shrouded in Secrecy, Agency Withholds Unclassified Information," *Washington Post,* May 29, 2004, p. A21.

[135] "NRC Initiates Additional Security Review of Publicly Available Documents; Temporarily Suspends Agency's On-Line Library," *NRC News,* Oct. 25, 2004, No. 04-135; Sean Madigan, "Documents Return to Online Nuclear Regulatory Library After Terror Review," *CQ Homeland Security,* Nov. 17, 2004. These were identified as such things as floor plans for university laboratories giving the location of equipment that uses nuclear materials and of storage facilities for them. (See, for example, M. Ahlers, "Blueprints for Terrorists? Sensitive Nuclear Info Ends Up on NRC Web Site," *CNN.Com* at [http://www/cnn.com/2004/US/10/19/terror.nrc/index.html]).

[136] Letter from Rep. Edward J. Markey to Hubert T. Bell, Inspector General, U.S. Nuclear Regulatory Commission, Mar. 21, 2005.

[137] Sean Madigan, "Nuclear Documents Back Online," *CQ Homeland Security,* June 10, (continued...)

task force concluded that the agency could withhold information that could be deemed useful to terrorists if the information were not already available to the public pursuant to its new Sensitive Information Screening Project, but FOIA principles needed to be followed to withhold information. The task force identified the precise kinds of information that could be withheld under the various FOIA exemptions.[138]

Also during this time period, the National Academies released an unclassified version of a report, that included among its findings that the commission's security restrictions on the sharing of information with industry and the public negatively affected "constructive feedback and cooperation. The committee recommended that the ... NRC improve the sharing of pertinent information on its security analyses of spent fuel storage with nuclear power plants operators and system vendors. More constructive interaction with the public and with independent analysts also could increase confidence in ... NRC and industry decisions and their actions to reduce the vulnerability of spent fuel storage to terrorist attacks."[139]

Controls on Unclassified Biological Research Information

Traditionally, open communication of biological information fosters the conduct of research and development. Also, emergency preparedness requires exchange of information to inform local health officials "... of what agents are being studied in their jurisdictions so they can prepare for any unlikely future events."[140] However, some biological information and data could pose a domestic or international security threat, which has led to federal controls.[141] For instance, a 2006 National Academies report described a variety of biotechnology agents and specific genetic advances that could be used in research and could increase the potential for biowarfare.[142] It also inventoried some dual-use biological agents and research developments that could

---

[137] (...continued)
2005. For original wording, see "NRC Task Force Report on Public Disclosure of Security-Related Information," Nuclear Regulatory Commission, May 18, 2005, approved June 30, 2005. [http://www.fas.org/sgp/othergov/nrc-disc.pdf].

[138] "NRC Task Force Report on Public Disclosure of Security-Related Information," NRC, May 18, 2005, approved June 30, 2005, originally cited in "NRC Adopts Policy on Disclosure of Security Information," *Secrecy News,* Aug. 16, 2005,

[139] "Spent Fuel Stored in Pools at Some U.S. Nuclear Power Plants Potentially at Risk From Terrorist Attacks; Prompt Measures Needed to Reduce Vulnerabilities," *NAS Press Release,* April 6, 2005. See also"Secrecy Impedes Security, National Academy Says," *Secrecy News,* Apr. 8, 2005; and the NAS report: *Safety and Security of Commercial Spent Nuclear Fuel Storage: Public Report,* by Committee on the Safety and Security of Commercial Spent Nuclear Fuel Storage, National Academy of Sciences Press, 2005.

[140] "Laura H. Kahn, "Biodefense Research: Can Secrecy and Safety Coexist?" *Biosecurity and Bioterrorism: Biodefense Strategy, Practice and Science,* vol. 3, no. 2, 2004, p. 4.

[141] For additional information, see CRS Report RL31695, *Balancing Scientific Publication and National Security Concerns: Issues for Congress*, by Dana Shea.

[142] Committee on Advances in Technology and the Prevention of Their Applications to Next Generation Biowarfare Threats, *Globalization, Biosecurity, and The Future of the Life Sciences*, National Academies Press, 2006, pp. 39-40.

be used malevolently. For example, "The same reverse genetic technologies that can be used to develop new vaccines against RNA viruses could also be used to construct modified viruses, including possibly viruses that express heterologous virulence factors that result in more lethal disease."[143] Ominously, it observed that

> [in] the past, dual-use concerns have focused on pathogens and on the challenges associated with controlling dangerous pathogens. As already emphasized, this committee's deliberations have indicated that the problem will be far broader and more profound in the future. For example, advances in neurobiology may make it possible to manipulate behavior and thought processes, while gene expression technologies just now coming to fruition will make it possible to activate endogenous molecules in the body — with possibly wide ranging and everlasting effects. Advances in synthetic biology and nanotechnology will offer similar rich opportunities for dual use. Nanodevices that may be used to unplug blocked arteries could instead be employed to interfere with circulatory function. Advanced drug delivery technologies and pharmacogenomics knowledge could be used to develop and deliver with greater efficiency new bioweapons, perhaps even selectively targeting certain racial or ethnic groups."[144]

To deal with concerns like these, some types of biological sciences information have already been controlled and proposals have been made to develop other types of governmental or nongovernmental systems to control access to information before research is conducted or in the prepublication phase. These proposals, which are discussed next, are not without controversy.

The federal government's regulation requiring the registration of laboratories that transferred certain "select agents" — organisms and toxins identified by the Centers for Disease Control and Prevention (CDC) as potentially useful in bioterrorist activities — began in 1996.[145] Registration of laboratories that possess such agents was mandated by P.L. 107-188, "The Public Health Security and Bioterrorism Preparedness and Response Act of 2002," enacted after the 9/11 attacks. The law requires coordination between the Department of Health and Human Services (DHHS) and the Department of Agriculture (USDA) to identify and regulate the use and transfer of such agents that pose a risk to public health, crops or livestock; registration of all facilities that use such agents; minimum safety requirements for registered facilities; background screening of persons using such agents; and a national database of such users. The USA PATRIOT Act, P.L. 107-56 prohibits access to select agents by certain persons, including certain immigrants, and persons with criminal or drug use history and other factors. Interim final regulations implementing these laws were issued in December 2002.[146]

---

[143] *Globalization, Biosecurity, and The Future of the Life Sciences*, op. cit., p. 53.

[144] *Globalization, Biosecurity, and The Future of the Life Sciences*, op. cit., p. 55.

[145] Pursuant to the Antiterrorism and Effective Death Penalty Act of 1996 (P.L. 104-132). For further information on this and subsequent activity, see CRS Report RL31719, *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness*, by Sarah A. Lister.

[146] The DHHS regulation is codified at 42 CFR Section 73.0, and the USDA regulation at (continued...)

National Science Advisory Board for Biosecurity. A National Academy of Sciences (NAS) report, *Biotechnology Research in an Age of Terrorism: Confronting the "Dual Use" Dilemma,* published in 2004 and dubbed the "Fink" report after the committee chairman, called for greater self-regulation by scientists, use of institutional biosafety committees at academic and research institutions to monitor research that could possibly aid terrorism, NIH review of certain types of research reports before they are published, and use of screening criteria in a prepublication review. Regarding private scientific publishing, the Fink report largely left it up to journal publishers to make decisions about prepublication review procedures for articles involving biological agents. The Fink report also urged creation of a new federal advisory board to guide nongovernmental researchers and to develop responsibility among scientists to control flows of biodefense information. But it did not propose governmental control of such research.

In March 2004, the DHHS announced its intent to create a National Science Advisory Board for Biosecurity (NSABB), which became funded in 2005. It is managed and staffed by the National Institutes of Health (NIH). The NSABB is chartered to have 25 voting nongovernmental members with a broad range of expertise in molecular biology, microbiology, infectious diseases, biosafety, public health, veterinary medicine, plant health, national security, biodefense, law enforcement, scientific publishing, and related fields. The NSABB also includes nonvoting ex officio members from 15 federal agencies and departments. It is supposed to advise federal departments and agencies regarding oversight of dual-use nonclassified biological research. The board's charter also includes work to develop national policies to communicate and publish sensitive research results, a code of conduct for life sciences researchers, training programs and materials to educate the community about biosecurity, and strategies to foster international collaboration to oversee dual-use life sciences research. NIH aims to use the committee's guidance to develop policies to require performer institutions that it funds to use Institutional Biosafety Committees (IBC), to educate researchers, to issue guidance, and to review and advise on specific experiments that might be misused or pose a threat to the public health or national security. Policy guidance will flow from the federal board to the institutional committees if there is uncertainty or disagreement regarding denial of an experiment. The NSABB met in June 2005 and November 2005; it will meet again in 2006.

During its first meeting, the board established five working groups to develop criteria to identify dual-use research; criteria to communicate results of dual-use research; a life sciences code of conduct; international perspectives on dual-use research; and guidance on chemical synthesis of bacterial and viral genomes.[147] Some discussants proposed that biologists should be licensed to conduct sensitive biological research, that codes of conduct would need to be certified, and that methods of assuring compliance among research institutions would need to be

---

[146] (...continued)
7 CFR Part 331 and 9 CFR Part 121.

[147] Janet Coleman, "NSABB Working Groups Will Begin Discussions Soon...," *Research Policy Alert,* July 5, 2005.

developed.[148] Some contended that if the scientific community did not develop methods of monitoring and protecting sensitive research, policy makers might develop and try to enforce more stringent controls that ultimately might prove to be unacceptable.[149] During the November 2005 meeting, the working groups gave progress reports and discussed developing guidelines, including the use of risk-based procedures.

Views on Adequacy of Biosecurity Protection Policies. Some critics say existing biosecurity protections are inadequate to prevent terrorists from obtaining and using biological information and suggest that stronger measures should be taken, such as creation of a network that interacts closely with intelligence and military agencies to prevent misuse of biological information.[150] Related to this, a 2006 National Academies report, concerned about how new developments in the life sciences coupled with rapidly advancing fields such as nanotechnology and materials science could prove to threatening, endorsed the free and open change of information in the life sciences to the maximum extent possible. However, it also recommended,

- creating statutorily an independent advisory group in the security community to strengthen scientific and technical expertise within the intelligence and security communities;
- adopting and promoting a "common culture of awareness and a shared sense of responsibility within the global communities of life scientists," including development of codes of ethics; and
- establishing, "... a decentralized, globally distributed network of informed concerned scientists who have the capacity to recognize when knowledge or technology is being used inappropriately or with the intent to cause harm"[151] and whose interventions could take the form of counseling or "... reporting such activity to national authorities when its appears potentially malevolent in intent."[152]

Other shortcomings in current policy have been identified. For instance, the scope of the DHHS's NSABB board has been faulted because it does not extend to privately funded research nor harmonize international standards.[153] Others criticize the select agent rules as inadequate and say federal regulations should be expanded to prevent unauthorized persons from possessing the DNA components of a select

---

[148] "Rules of Engagement," *Nature*, July 7, 2005, p. 2.

[149] Eugene Russo, "New Biosecurity Panel Struggles With Role in Monitoring Sensitive Research," *Research Policy Alert*, July 5, 2005. See also Jeffrey Brainard, "National Biosecurity Board Holds First Meeting, Ponders Limits on Research," *Chronicle of Higher Education*, July 1, 2005.

[150] Russo, July 6, 2005, op. cit

[151] *Globalization, Biosecurity, and the Future of the Life Sciences*, op. cit., p. 8.

[152] *Globalization, Biosecurity, and the Future of the Life Sciences*, op. cit., p. 9.

[153] Jennifer Couzin, "U.S. Agencies Unveil Plan for Biosecurity Peer Review," *Science*, Mar. 12, 2004, citing Elisa Harris of the University of Maryland's Center for International and Security Studies.

agent.[154] George Church, a genetics professor at Harvard, reportedly "is organizing a consortium of researchers and academics to push the federal government to license anyone interested in purchasing DNA segments for agents of bioterror."[155] Similarly, John Steinbruner and colleagues at the Center for International and Security Studies at Maryland (CISSM), in a 2005 report, advocated mandatory licensure of researchers and institutions that conduct biodefense research. Three levels of independent review — at the institutional, national, and international level — would monitor risks and benefits of research proposals and would issue approval or disapproval for conduct of researchers and publications.[156]

Nongovernmental professional groups have explored the use of codes of conduct or self-policing policies[157] for research topics and publications. Some publishers adopted a set of voluntary, risk-based publishing principles, called "Statement of Scientific Publication and Security," 2003; but this, reportedly, has resulted in changes in only very few articles before publication.[158] In June 2005, the American Society for Microbiology drafted a code of ethics for its members and urged them to report to "appropriate authorities" misuses of microbiology information.[159] The Interacademy Panel on International Issues, consisting of most of the world's national science academies, issued a set of principles that urged scientists to take responsibility to prevent misuse of their work.[160] Two researchers, Margaret A. Somerville of McGill University and Ronald M. Atlas, President of the American Society for Microbiology, proposed an international code of ethics to

---

[154] Caitlin Harrington, "Lab-Synthesized Diseases Open a New Front in Bioterror War," *CQ Homeland Security,* Aug. 2, 2004.

[155] Harrington, op. cit.

[156] Eugene Russo, "Biodefense Research Needs Formal Oversight and Licensure - University of Maryland Report," *Research Policy Alert,* Feb. 22, 2006, citing John Steinbruner, et al., *Controlling Dangerous Pathogens: A Prototype Protective Oversight System,* University of Maryland, 2005.

[157] According to Dana Shea, CRS, for a representative list of codes of ethics developed by professional groups, see online at [http://www.biosecuritycodes.org/codes_archive.htm].

[158] Reportedly, the statement of policy was adopted by science journal editors and released on Feb. 15, 2003, and was published in *Science*, *Nature*, and the *Proceedings of the National Academy of Sciences*. It is available at [http://www.fas.org/sgp/news/2003/02 /sci021503.html]. For additional information, see CRS Report RL31695, op. cit. It has been reported that, according to an article published in 2003, "... the American Society of Microbiology (ASM) flagged two out of fourteen thousand articles as unsuitable for publication, and both of these papers were likely to be published after changes were made....(*The Unintended Audience: Balancing Openness and Secrecy: Crafting an Information Policy for the 21st Century*, op. cit., p. 39).

[159] Eugene Russo, "Biosecurity Advisory Board Considers Code of Ethics," *Research Policy Alert,* July 6, 2005.

[160] Shirley Haley, "Scientists Must Take Responsibility for Preventing Misuse of Their Work — Interacademy Panel," *Research Policy Alert,* Dec. 6, 2005. The document is "IAP Statement on Biosecurity," Nov. 7, 2005.

prevent bioterrorism.[161] Adherents to the code would refuse to conduct work that could be used in bioterrorism and would seek to restrict access of those they believe could use information maliciously.

It was noted above in the section on "Nongovernmental Experts' Recommendations To Use Risk Analysis To Identify and Control Sensitive Information," that proposals have been made to instill in researchers a culture that discourages research that could be used malevolently, that professional peer reviews should be conducted before publication of work that should be protected, and that the federal government should define policy controls for these activities. In addition, J. Gaudioso and R. M. Salerno proposed a biosecurity risk assessment process that would restrict the use of agents that have the potential to be weaponized and that could serve as the basis for international standards. This process would involve using

> four Biosecurity levels: low, moderate, high, and extreme risk. The overwhelming majority of pathogens and toxins would fall into the low-risk category (requiring practices such as locking unattended laboratories and maintenance of documentation of agents used), and most select agents would be

---

[161] Margaret A. Somerville and Ronald M. Atlas, "Ethics: A Weapon to Counter Bioterrrorism," *Science*, Mar. 25, 2005, pp. 1881, 1882. The proposed code is: "In order to prevent the life sciences from becoming the death sciences through bioterrorism or biowarfare, all persons and institutions engaged in all aspects of the life sciences must: "1. Work to ensure that their discoveries and knowledge first do no harm: I) by refusing to engage in any research that is intended to facilitate, or there is a high probability of its being used to facilitate bioterrorism or biowarfare, both of which violate the fundamental moral values of humanity; and ii) by complying with the prohibition of the Biological Weapons Convention to never, under any circumstances, knowingly or recklessly contribute to the development, production or acquisition of microbial or other biological agents or toxins, whatever their origin or method of production, of types or in quantities that cannot be justified on the basis of their being necessary for prophylactic, protective, therapeutic, or other peaceful purposes. 2. Work for the ethical and beneficent advancement, development and use of scientific knowledge. 3. Call to the attention of the public, or the appropriate persons or bodies, activities, including unethical research, that there are reasonable grounds to believe are likely to contribute to bioterrorism or biowarfare. 4. Take reasonable care to assure biosecurity by seeking to allow access to biological agents that could be used as biological weapons only to individuals who there are reasonable grounds to believe will not misuse them. 5. Seek to restrict the dissemination of dual-use information and knowledge to those who need to know in cases where there are reasonable grounds to believe that there are serious risks that information or knowledge could be readily misused to inflict serious harm through bioterrorism or biowarfare. 6. Subject research activities to ethics and safety reviews and monitoring to establish their ethical acceptability: I) to ensure that legitimate benefits are being sought and that they outweigh the risks and harms; and ii) if human or animal subjects are involved, to ensure that such involvement is ethical and essential for carrying out highly important research. 7. Abide by laws and regulations that apply to the conduct of science unless to do so would be unethical, and recognize a responsibility to work through relevant societal institutions to change those laws and regulations that are in conflict with ethics. 8. Recognize all persons' rights of conscientious objection to participation in research that they consider ethically or morally objectionable and to refuse to participate without penalty. 9. Faithfully transmit the duties and obligations embodied in this code, and the ethical principles upon which it is based to all who are, or may become, engaged in the conduct of science."

> placed in the moderate-risk category (requiring additional safeguards such as access controls and personnel checks). The security measures for low-and moderate-risk categories should pose reasonable costs and largely rely on existing biosafety measures. Very few agents would be designated high risk (requiring more stringent security measures and a dedicated Biosecurity officer). Perhaps only variola major, because it is no longer found in nature would be considered an extreme risk, requiring the most stringent protections (such as comprehensive background investigations and an on-site guard force). Higher security than that currently mandated by federal regulations would only be applied for those very few agents that represent true weapon threats. Biosecurity levels should be developed and vetted by experts in biological weapons, microbiology, security, and public and agricultural health. This would help federal agencies apply uniform criteria to grantees and could form the basis for standardizing biosecurity internationally.[162]

Brian J. Gorman proposed a risk-based alternative approach for prepublication peer review. He called for a risk-based process called "Due Process Vetting System" (DPVS) together with "... a Risk Assessment Scale [RAS] and a Least Restrictive Classification System for the communication, assessment, and disposition of sensitive life science research in a manner consistent with national security interests."[163] The process would be overseen by a new agency called the Biologic Regulatory Commission, modeled after the Nuclear Regulatory Commission. The vetting process would be triggered at the request of an author or peer reviewer if an article attained a predetermined score on the RAS set by the BRC. "The RAS surveys opinions of informed reviewers including the author of the article, the author's Institutional Review Board or Institutional Biosafety Committee (IBC), and finally the journal interested in publishing the article."[164] The DPVS would safeguard high-risk articles by providing the government with a mechanism to identify "potentially dangerous articles before they reach the presses,"[165] would avoid the "deleterious

---

[162] Jennifer Gaudioso and Reynolds M. Salerno, "Biosecurity and Research: Minimizing Adverse Impacts," *Science*, Apr. 30, 2004, citing J. Gaudioso and R. M. Salerno, "A Conceptual Framework for Biosecurity Levels," *BTR 2004: Unified Science and Technology for Reducing Biological Threats and Countering Terrorism — Proceedings*, Albuquerque, NM, March 18-19, 2004.

[163] Brian J. Gorman, "Balancing National Security and Open Science: A Proposal for Due Process Vetting," *Yale Journal of Law and Technology*, 2005, pp. 2, 15.

[164] Gorman, op. cit., pp. 28-29. The proposed survey would use a five-level scaling technique that would generate a risk score. The survey would "...address the degree to which the prospective article presents danger to human life, livestock, and agriculture on several axes." Survey questions would focus on whether the paper would present a risk to society, render a vaccine ineffective, contribute to increasing resistance to antibiotic or antiviral agents, lead to increased virulence of a pathogen, increased transmissability of a pathogen, alter the host range of a pathogen, permit evasion of diagnosis or detection, or contribute to weaponization of a biological agent (Gorman, pp. 33-34). It would also assess the potential for a "malevolent actor" to "use the science in question," the extent of damage from misuse, and the potential for publication of the material to promote "conversion of benign" already published articles to more sensitive status (Gorman, pp. 35-37).

[165] Gorman, op. cit., pp. 21-22

effects of censorship,"[166] and would make articles available only to a "select academy of biodefense researchers after the authors, the publishing journal and others, reach a consensus with the government through cooperative vetting of the article in question."[167] Gorman proposed expanding the academy to a qualified body of world scientists, an approach he said is superior to the ASM model and ad hoc approaches undertaken by the majority of U.S. biosciences journals.[168]

Some scientists disagree with the types of aforementioned restrictions. Existing controls on "select agents," reportedly, have caused " ... many researchers ... to discontinue or not pursue research on regulated biological agents, rather than implement the new security regulations and bear the associated financial burden. Reportedly, the CDC expected 817 entities to register under the new select agent rule. Instead, only 323 facilities are registered with the CDC, which indicated that many institutions have discontinued their work with select agents."[169] There are also complaints that U.S. "select agent" rules can hinder cooperation from foreign scientists who cannot afford security controls and that many foreign laboratories do not meet the standards for conducting such research demanded by the U.S. government. As a result, foreign partners, some charge, may be forced to become "mere sample exporters," and criminal sanctions might be applied to the U.S. partner in a foreign collaboration if the foreigner partner's laboratory does not meet U.S. research security standards.[170] Complaints about the CDC's "information security" manual have led to concern by influenza researchers that the CDC is not releasing databases of virus sequences and other data needed to develop flu vaccines, thereby potentially damaging the development of public health protections.[171]

In addition, at the first NSABB meeting, some members suggested that instead of formal restrictions, ethics education for researchers would suffice to deal with potential problems.[172] Others suggest that controls on biological research information could constrain the exchange of information needed to develop effective defenses against dangerous pathogens.[173] A National Academies' report, *Seeking Security; Pathogens, Open Access and Genomic Data Bases,* published in 2004, that had been requested by the National Science Foundation and the Central Intelligence Agency, concluded that there should be no change in current policies that allow scientists and

---

[166] Gorman, op. cit., p. 21.

[167] Gorman, op. cit., p. 21.

[168] Gorman, op. cit., pp.23, 43.

[169] See Gaudioso and Salerno, "Biosecurity and Research: Minimizing Adverse Impacts," *Science,* Apr. 30, 2004, op. cit. For additional information, see CRS Report RL31719. op. cit.

[170] Richard Stone, "Select Agents: Heightened Security or Neocolonial Science?," *Science,* Dec,. 24, 2004.

[171] Rebecca Carr, "CDC Locks Up Flu Data," *The Atlanta Journal-Constitution,* Oct. 3, 2005.

[172] "Rules of Engagement," op. cit.

[173] Laura Donohue (fellow at the Center for International Security and Co-operation), "Censoring Science Won't Make Us Any Safer, *The Washington Post,* June 26, 2005, p. B05

the public unrestricted access to genome data on microbial pathogens. Access, it concluded, improves the nation's ability to fight both bioterrorism and naturally occurring infectious diseases.[174] Open access to raw sequence data is unlikely to help bioterrorists develop weapons, and preventing distribution of such information could hurt research to prevent bioterrorism and emerging diseases such as severe acute respiratory syndrome (SARS). Genomic information about most dangerous pathogens is already available, it said, and if the government wants to restrict distribution of information in the future, such information should be classified. The report concluded that security against bioterrorism would be achieved best by policies that facilitate, not limit, the free flow of this information. In May 2005, the DHHS attempted to prevent the National Academy of Sciences from publishing an article in the *Proceedings of the National Academy of Sciences* on how the U.S. milk supply could be tainted with botulism and control measures to prevent it. The Academy published it on the grounds that the benefits of publishing the paper giving biodefense guidance outweighed any threats.[175]

Other nations and international scientific groups have addressed this issue. For instance, reportedly a December 13, 2004 paper issued jointly by the United Kingdom's Royal Society and the Wellcome Trust urged caution on government intervention. The joint paper said "government should ask scientific societies and funding institutions to take more responsibility for vetting and preventing the dissemination of risky technical details. The paper suggested that grant review forms could include a check box for bioterror issues to ensure that they are considered."[176] Also, at a meeting in June 2005 in Geneva, life scientists from several countries sought to develop a code of conduct. Biosafety in life sciences research was also a topic of discussion at an Organization for Economic Cooperation and Development (OECD) International "futures" program meeting in September 2004, and the National Academies held an International Forum on Biosecurity in Como, in March 2005 to discuss convergence on codes of conduct and oversight of biosecurity research.[177]

Issues Dealing with Geospatial Information

There is considerable controversy about providing access to certain types of geospatial information, including satellite imagery and maps depicting ordinary

---

[174] The report is *Seeking Security: Pathogens, Open Access, and Genome Databases*. Cited in David Malakoff, "Report Upholds Public access to Generic Codes," *Science,* Sept. 17, 2004.

[175] Kelly Field, "Federal Officials Ask National Academy of Sciences Not to Publish Paper on Bioterrorism," *Chronicle of Higher Education,* June 6, 2005; Richard Monastersky and David Glenn, "National Academy of Sciences Publishes Paper that U.S. Calls 'Road Map for Terrorists,'" *Chronicle of Higher Education,* July 8, 2005.

[176] Eliot Marshall, "Biodefense: Experts Warn Against Censoring Basic Science," *Science,* Dec. 17, 2004.

[177] Janet Coleman, "Dual Use International Dialogue Hampered by Lack of Recognition of Biosecurity Risk," *Research Policy Alert,* July 11, 2005.

geographic features, buildings, sensitive facilities, hazardous materials storage facilities, and so forth.

Supporting more open access to such information, in March 2004, the RAND Corporation released a study recommending that the federal government should not remove geospatial information such as maps and imagery from public availability because much of it is not current enough to meet terrorists' needs, terrorists can obtain such information from other sources, and the public benefits from access to much federal geospatial information. Instead, it recommended that the federal government develop an analytical process to assess the potential homeland security sensitivity of specific publicly available geospatial information using three filters: usefulness, uniqueness, and societal benefits and costs.[178] Subsequently, in June 2005, the Homeland Security Group of the Federal Geographic Data Committee, an 18-member federal interagency group that coordinates geospatial data, issued for consideration interim[179] and then final guidelines for public, private, and nonprofit organizations that originate and publicly disseminate geospatial data.[180] The guidelines seek to balance "security risks and the benefits of geospatial data dissemination" and suggest how organizations can use risk-based procedures to provide access to data while protecting sensitive information. The group observed that safeguarding is justified only for data that contain sensitive information that is difficult to observe and not available from open sources, that are the unique source of the sensitive information, and for which the security risk outweighs the societal benefit of dissemination. Two options were offered to handle sensitive data before public release — changing it to remove or modify the sensitive information by summarizing it, blurring details, and so forth; or restricting the data but maintaining it in original form and making it available to those who need it, such as first responders.[181]

Congressional action in 2004 tightened controls on some geospatial information. Section 914 of P.L. 108-375, the Defense Authorization Act FY2005, signed on October 28, 2004, authorized a new FOIA exemption three category permitting the withholding from public disclosure of land remote sensing information prohibited from sale to nongovernment or government-approved customers for reasons of national security and under license as described by the Land Remote Sensing Policy Act of 1992, (15 U.S.C. Section 5601 et seq.). Such information may not be

---

[178] John C. Baker, et al., *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information*, Prepared for the National Geospatial-Intelligence Agency, RAND National Defense Research Institute, 2004, pp. xvii-xxxiv.

[179] "Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concern," Sept. 7, 2004, available at [http://www.fgdc.gov/fgdc/homeland /revised_access_guidelines.pdf]. A companion document that summarizes significant comments received during the public review and responses to the comments is available at [http://www.fgdc.gov/fgdc/homeland/response_to_comments.pdf].

[180] U.S. Geological Survey, Federal Geographic Data Committee, *Final Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns*, June 2005. Available at [http://www.fgdc.gov].

[181] *Final Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns*, op. cit., pp. 1-2.

exempted from disclosure to Congress; information disclosed to state or local government may not be made available to the public; and agencies are required to protect such information from disclosure. On November 18, 2004, the DOD's National Geospatial Intelligence Agency (NGA) announced that for security reasons, as well as for reasons of potential intellectual property rights violations for information gathered commercially in other countries, it would "... remove its Flight Information Publications (FLIP), Digital Aeronautical Flight Information File (DAFIF), and related aeronautical safety of navigation digital and hardcopy publications from public sale and distribution."[182] After the review of comments was completed in November 2005,[183] the agency implemented its plan. However, its rationale for removal of information focused exclusively on the intellectual property rights issue, not the security dimensions.[184]

In contrast to restraining information, legislation has been introduced to expand use and applications of federal remote sensing data. During the 109th Congress, H.R. 426, "Remote Sensing Applications Act of 2005," reported favorably on June 27, 2005 (House Report 109-157), would, among other things, direct the Administrator of the National Aeronautics and Space Administration (NASA) to establish a program of grants for pilot projects to explore the integrated use of sources of remote sensing and other geospatial information to address state, local, regional, and tribal agency needs. It requires the Administrator, when awarding grants, to give preference to specified types of projects. The bill did not contain language constraining use of data.

The Department of Homeland Security's SBU Directives

The DHS issued an internal management directive (MD 11042) on *"Safeguarding Sensitive But Unclassified (For Official Use Only) Information"* on May 11, 2004, to safeguard SBU information within DHS. Such information would be labeled For Official Use Only (FOUO)[185] and would be defined "to identify

---

[182] The agency's notice of rulemaking said it sought to accomplish the following objectives: "safeguarding the integrity of Department of Defense (DOD) aeronautical navigation data currently available on the public Internet; preventing unfettered access to air facility data by those intending harm to the United States, its interests or allies; upholding terms of bi-lateral geospatial data-sharing agreements; avoiding competition with commercial interests; and avoiding intellectual property/copyright disputes with foreign agencies that provide host-nation aeronautical data" (National Geospatial-Intelligence Agency (NGA), Department of Defense, "Modification to Announcement of Intent To Initiate the Process To Remove Aeronautical Information From Public Sale and Distribution," *Federal Register*, Dec. 17, 2004, vol. 69, no 242, pp. 75517-75518).

[183] See the release at [http://www.nga.mil/NGASiteContent/StaticFiles/OCR/nga0509.pdf].

[184] "The National Geospatial-Intelligence Agency To Go Forward with Proposal to Remove Aeronautical Data from Public Access Release," NGA press release no. 05-17, Nov. 29, 2005, [http://www.fas.org/sgp/news/2005/11/nga112905.html].

[185] DHS, *Safeguarding Sensitive But Unclassifed (For Official Use Only) Information*, (continued...)

unclassified information of a sensitive nature, not otherwise categorized by statute or regulation the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest." Portions of the memorandum generated considerable opposition because of its mandatory and punitive employee and contractor nondisclosure requirements. In January 2005, the controversial requirements were replaced with requirements to educate employees in security practices, and the document was reissued as MD 11042.1.[186] Contractors are still required to sign nondisclosure agreements, and DHS employees and contractors are still subject to administrative or disciplinary action for violating the policies.[187]

The directive identified several types of control labels that could be SBU, including FOUO, CII, and SSI and so forth and 11 types of sensitive unclassified information that can be designated for official use only (FOUO) — a type of SBU — by any DHS employee, consultant, or contractor. The list includes one clearly identifiable technology-related item, which conceivably might include the results of DHS-sponsored or conducted scientific research and development:

---

[185] (...continued)
MD11042, May 11, 2004, available at [http://www.dhs.gov/interweb/assetlibrary/Mgmt_NEPA_MD11042SensUnclass.pdf]).

[186] In Aug. 2004, DHS promulgated requirements for its employees and contractors to sign a nondisclosure agreement to handle and protect PCII, SSI and other "other SBU" nonclassified information. Among its provisions, it stated that penalties for violation could include "administrative, disciplinary, civil, or criminal action," and that signing the nondisclosure agreement also allows the government "to conduct inspections, at any time or place, for the purpose of ensuring compliance" *(DHS Non-disclosure Agreement*, DHS Form 11000-6 (08-04). Some federal employee unions criticized the requirement saying that it duplicated regulations that protect certain types of information, ("Homeland Security," *Washington Post*, editorial, Dec. 3, 2004, p. A26), that it imposed criminal prosecution for disclosing information that is to be made available under FOIA, that it infringed on of free-speech rights (Eileen Sullivan, "Searchers and Gag Orders: Homeland Security's Unprecedented Campaign Cloaks Unclassified Info," *FederalTimes.com*, Dec. 6, 2004), and that it would allow "... officials to suppress and cover up evidence of their own misconduct or malfeasance by stamping documents 'for official use only....'"Sullivan, op. cit.) It was reported that congressional staffers had been asked, and refused, to sign such statements on the grounds that they need to oversee the agency (Chris Strohm, "Homeland Security Reverses Secrecy Policy But Protests Persist," *Gov Exec.com*, Jan. 12, 2005).

[187] Regulations for DHS contractors to sign nondisclosure agreements for access to sensitive but unclassified information appear in DHS's Supplement to the Federal Acquisition Regulation (FAR), sec. 3037.103-71, "Conditional Access to Sensitive But Unclassified Information." It was reported that DHS required participants in an unclassifed workshop it sponsored at Booz Allen Hamilton on "Anticipating the Unanticipated," "to consider novel weapons and tactics that might be employed by terrorists," to sign a nondisclosure agreement (Steven Aftergood, "More Non-disclosure Agreements for Unclassified Info," *Secrecy News*, Dec.1, 2004). See also Chris Strohm, "Homeland Security Reverses Secrecy Policy But Protests Persist," *Gov Exec.com*, Jan. 12, 2005; "Homeland Security Officials End Workers' Pledge of Secrecy," *Technology Daily, AM Edition*, Jan. 13, 2005; "Homeland Security," *Washington Post*, editorial, Dec. 3, 2004, p. A26.

> (k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system.[188]

P.L. 107-296 specified that, if "practicable," DHS's research is to be unclassified, but the Presidential signing statement may have mitigated this provision.[189] It remains to be seen how this SBU regulation will affect information generated by DHS-funded research and development grants and contracts, and what the response will be of universities that conduct research for DHS under its academic centers of excellence programs.

Access to the information covered by the DHS SBU directive is on a "need-to-know" basis, and information can be shared with cleared homeland security personnel at state and local levels. The directive said the use of the FOUO designation did not automatically exempt information from disclosure under FOIA but "[i]nformation requested by the public under a FOIA request must still be reviewed on a case-by-case basis." The information would retain the FOUO designation until the originator or other officials determine otherwise. Procedures to protect and disseminate such information outside of DHS were spelled out, including requirements for secure storage and suggestions for encrypted Internet and telephone communications. Some other agencies also require employees to sign

---

[188] The other items in the list are (a) information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments; (b) information exempt from disclosure per 5 U.S.C. 552a, Privacy Act; (c) information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements; (d) other international and domestic information protected by statute, treaty, regulation or other agreements; (e) information that could be sold for profit; (f) information that could result in physical risk to personnel; (g) DHS information technology (IT) internal systems data revealing infrastructure; (h) systems security data revealing the security posture of the system; (I) reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities; and (j) information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security (MD 11042 Issue Date: 5/11/2004, Revised as MD 10042.1, Jan. 2005, op. cit., available at [http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf]).

[189] Section 306(a) of P.L. 107-296 provides that "to the greatest extent practicable, research conducted or supported by the ... DHS shall be unclassified." However, "President Bush's signing statement ... states that the executive branch will 'construe and carry out' this section, and other provisions of the law, including those addressing information analysis and infrastructure protection, 'in a manner consistent with the President's constitutional and statutory authorities to control access to and protect classified information, intelligence sources and methods, sensitive law enforcement information, and information the disclosure of which could otherwise harm the foreign relations or national security of the United States.'" From [http://www.whitehouse.gov/news/releases/2002/11/print/20021125-10.html], as] cited in U.S. Library of Congress, Federal Research Division, *Laws and Regulations Governing the Protection of Sensitive But Unclassified Information. A Report Prepared ... Under an Interagency Agreement with the NASA Office of Inspector General.* Project Manager: Alice R. Buchalter, Sept. 2004, p. 8.

nondisclosure agreements in order to protect SBU information.[190] (See below in the section labeled "Critique of Nondisclosure Requirements.")

Contentious Issues, Together With Legislative Action and Other Options

The need to balance security and access poses a dilemma for policymakers that was captured in the text of a joint report prepared in December 2004 by the Heritage Foundation and Center for Strategic and International Studies. The report noted that "[I]t is necessary to strike the right balances in sharing information with or withholding information from the public. Policies that are either overly neglectful or overzealous ill serve efforts to enhance homeland security."[191] Some critics contend that many government-instituted controls on sensitive information, or on scientific and technical information, may be unwarranted. For instance, *OMB Watch*, an interest group newsletter that advocates more access to information, maintains an inventory and website that lists information that federal and state agencies have removed from public access for security reasons.[192] In March 2005, Steven Aftergood, the editor of *Secrecy News*, published online by the Federation of American Scientists, catalogued information deleted, sometimes, he contends, inappropriately, from government files or to which public access has been denied. This information includes unclassified technical reports from the Los Alamos National Laboratory, 30- to 50-year old historical records at the National Archives, orbits of Earth satellites, aeronautical maps, and data previously available from the National Geospatial Intelligence Agency.[193]

Some of the critiques of information control policies in specific scientific and technical arenas have already been described in this report. In addition, a number of criticisms have been made that cut across sensitive information controls broadly and may influence decisions about balancing security and access to sensitive unclassified information. These criticisms, which are discussed next, focus on allegations that some controls can exacerbate vulnerability or stifle scientific research and technological innovation; vagaries in nondisclosure requirements; the relationship of SBU to FOIA; inconsistency in agencies' definitions of and processes to identify SBU information; developing a standard definition of SBU information; monitoring agency use of risk-based standards for SBU; and recommendations for better governance of SBU information procedures. These sections also identify legislation that has been introduced and action Congress has taken on some of these issues.

---

[190] Eileen Sullivan, "Searches and Gag Orders: Homeland Security's Unprecedented Campaign Cloaks Unclassified Info," *Federal Times*, Dec. 6, 2004, "Homeland Secrecy," *Washington Post*, Dec. 3, 2004, p. A26.

[191] James Jay Carafano and David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, Heritage Foundation Special Report SR-02, Dec. 13, 2004, pp. 20-21.

[192] Available at [http://www.ombwatch.org/article/articleview/213#agency].

[193] Steven Aftergood, "The Age of Missing Information," Mar. 17, 2005, available at [http://slate.msn.com/id/2114963/].

Allegations That Some Controls Can Exacerbate Vulnerability and Stifle Scientific Research and Technological Innovation

Sensitive information controls may protect vulnerable buildings and public services from terrorist threats, but some critics allege that preventing access to such information can exacerbate vulnerabilities and stifle the development of innovations to enhance protection. According to one critic,

> A large sign in New York City, indicating the location of a natural pipeline was taken down after a website posted a photograph of the sign.... Although federal regulations require that the location of natural gas lines be made as obvious as possible to the public for safety reasons, the company that owns the pipeline asserted that local laws allowed the sign's removal. ... The regulations requiring that natural gas pipelines be clearly marked were established to prevent accidental rupture that often causes injuries an deaths to residents, contractors, and energy responders. Ironically, removing such information puts the public in greater danger of lethal accidents.[194]

Some say that protections on information access and dissemination are especially burdensome to scientific research and academic research and that the scientific community's potential to generate knowledge and innovations to assist in combating terrorism could be compromised by overzealous information security controls. For instance, "[t]errorists will obtain knowledge," one critic emphasized.[195] "Our best option is to blunt their efforts to exploit it. Keeping scientists from sharing information damages our ability to respond to terrorism and to natural disease, which is more likely and just as devastating. Our best hope to head off both threats may well be to stay one step ahead."[196]

On October 18, 2002, the three presidents of the National Academies issued a statement that 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 government policy 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. "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 that could possibly be of use to potential terrorists. An American Civil Liberties Union (ACLU) report addressing governmental restrictions on science, observed that "[t]he 'sensitive but unclassified' and equivalent categories that effectively bar public access to information must be

---

[194] "Security Measures Invoked to End Safety Measures," *OMB Watch*, Sept. 7, 2004.

[195] Donohue, op. cit., p. B05.

[196] Donohue, op. cit., p. B05.

eliminated. All information should either be properly classified or unrestricted."[197] Similarly, the American Association of University Professors recommended, "We should resist or seek to repeal efforts to regulate unduly, or to make secret, the results of lawful research projects under novel uses of the "sensitive but unclassified" rubric."[198] The National Academies held a workshop on this subject early in 2003, in cooperation with the Center for Strategic and International Studies. Subsequently, the CSIS and the Academies established a "Roundtable on Scientific Communication and National Security," a working group composed of scientific and security leaders that will hold continuing discussions to try to develop a workable publications policy. (For additional information, see the aforementioned CRS Report RL31845.)

A legal author argued that including SBU information clauses in contracts is "constitutionally suspect," especially with regard to university-conducted research that is supported as an essential public good. Use of the term SBU raises "... the possibility of government censorship of private speech ... the primary danger addressed by the Free Speech Clause,"[199] and imposes "... a prior restraint on private speech,"[200] even though there may not be enough of a threshold level of national Security danger to overcome the right to free speech. These considerations,

> ... suggest ... that SBU secrecy controls that reach into university discourse pose a particular danger because of the special role of the university in promoting innovation and expression outside of government control and because, with respect to scientific information in particular, the university has a special role in conducting research for the purpose of expansion and dissemination of knowledge. Although the government shapes expression on university campuses in many ways, the expectation is that expression not identified as the Government's will be unconstrained. The special role of the university thus must weigh in the constitutional balance.[201]

According to this author, government may have a legitimate constitutional right to protect SBU information in contracts, if there is sufficient national security reason, if uniform definitions linked to specific levels of national security danger are used, if there are review procedures, and if the method used to control information is the least restrictive necessary to fulfill the government's legitimate interests.[202]

Some say that placing controls on unclassified information could negatively affect government relations with the private sector and procurement for information

---

[197] ACLU, *Science Under Siege*, op. cit., p. 32.

[198] *Academic Freedom and National Security in a Time of Crisis*, American Association of University Professors Special Committee on Academic Freedom and National Security in a Time of Crisis, Oct. 2003.

[199] Leslie Gielow Jacobs, "A Troubling Equation in Contracts for Government Funded Scientific Research: 'Sensitive But Unclassifed' = Secret But Unconstitutional," *Journal of National Security Law and Policy*, 2005, p. 127.

[200] Jacobs, op. cit., p. 128.

[201] Jacobs, op.cit., p. 156.

[202] Jacobs, op. cit., pp. 157-159.

technology and other contracts. New ideas for information security technologies, including hard technology, software and biotech-related products, often come from overseas, as do bids for contracts to handle sensitive agency information. Reportedly, foreign vendors will have trouble complying with contracts that need to meet information security standards. It has been reported that requests for proposals (RFPs) coming from the Defense Security Services involving data processing for its SBU information say that employees of potential vendors need to be U.S. citizens, with background checks. DHS and DOT procurement rules involving sensitive information specify background checks for prime or subcontractors and that nondisclosure forms have to be signed.[203]

Critique of Nondisclosure Requirements

A number of agencies require employees, contractors, and users of sensitive information to sign nondisclosure agreements or impose penalties for disclosing SBU and related information. Some critics contend that language relating to penalties is often vague, varies from agency to agency, and that some agencies' mandatory nondisclosure provisions and associated penalties for disclosure might weaken federal employee rights and whisteblower protections. Some agencies' policies are illustrated in **Appendix A** and elsewhere in this report. For example, nondisclosure agreements are authorized in P.L. 107-296 relating to sharing of SHSI with state and local government personnel (sec. 892) and for handling SSI (sec. 1601). Section 214 of the law allows penalties consisting of imprisonment, fines, administrative penalties or dismal from employment for employees of DOT and DHS who inappropriately share CII information. DHS Management Directive 11042.1 prescribes penalties consisting of administrative or disciplinary actions for DHS employees and contractors for disclosing SBU information. DHHS has nondisclosure provisions and penalties for disclosure of select agent information and other sensitive information, as does the CDC for SBU information and the USDA, for sensitive information. The Department of the Treasury requires that certain bidders sign nondisclosure agreements for SBU information.[204] The Department of Energy (DOE) and the Nuclear Regulatory Commission (NRC) may penalize unauthorized release of certain types of SBU information and unclassified nuclear information. In addition, users of federal SBU information exchange systems are subject to nondisclosure provisions and usually are required to have clearances to view such information. (For details, **see Appendix B** to this report.) The General Services Administration attaches to business solicitations detailed explanation of how its bidding documents will be available only to authorized firms that have completed forms allowing them access to "sensitive but unclassified" bidding information. Such firms need to complete a document attesting that they will

---

[203] Alison Diana, "Law Expert Marcia Madsen on the Government IT Goldmine," *Technewsworld*, Mar. 5, 2004.

[204] For example, Department of the Treasury, "Solicitation TIRNO-04-R-00001, Conditional Access to Sensitive but Unclassified Information Non-disclosure Agreement," [for a Treasury Communications Enterprise (TCE) procurement].

undertake reasonable care, and limit dissemination to authorized users who have a "need to know."[205]

Penalties for disclosing SBU information can be more punitive than for disclosing classified information according to J. William Leonard, the director of the Information Security Oversight Office, (ISOO) at the NARA:

> For example, should a Federal employee disclose certain unclassified information - specifically Critical Infrastructure Information - in an unauthorized manner, that individual now is subject to criminal sanctions under Section 214(f) of the Homeland Security Act. At the same time, an unauthorized disclosure of certain types of classified information by that same employee would not necessarily be subject to criminal sanctions. The reason for such disparity is not readily apparent.[206]

The Project on Government Oversight, a watchdog group, criticized the revised DHS employee nondisclosure policy released in January 2005, saying it is "still problematic" because DHS "... prevents employees from disclosing information that is available to the public under the Freedom of Information Act [FOIA]."[207]

Legislation Introduced Affecting Disclosure Policies. Legislation has been introduced which may be responsive to some of these concerns. S. 494, "The Federal Employee Protection of Disclosures Act," which was reported without amendment on May 25, 2005 (Senate Report 109-72), would among other things protect any federal employee who lawfully discloses evidence of waste, abuse or mismanagement, including disclosure of classified information if made to Members of Congress or staff authorized to receive it. It also would authorize the Merit Systems Protection Board to review charges for retaliation for whistleblowing; require all agency nondisclosure forms to contain language preserving the right of federal employees to disclose certain information, and amend the Homeland Security Act of 2002 to allow federal employees to disclose independently obtained critical infrastructure information for specified whistleblower purposes. The House version of the "Federal Employee Protection of Disclosures Act," H.R. 1317, which was ordered to be reported amended without written report on September 29, 2005, and related bill, H.R. 3097, would protect any federal employee who lawfully discloses what he or she believes is credible evidence of waste, abuse, or gross mismanagement, without restriction as to time, place, form, motive, context, or prior disclosure. Exempt under H.R. 1317, would be information held by the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, and the National Security Agency.

S. 888, introduced on April 21, 2005, "Homeland Security Information Guidance and Training Act of 2005," and referred to the Committee on Homeland

---

[205] See, for example "Z — Chiller Replacement, Christie and Federal Bldg., Huntington, WV," *FPO Daily, May 22, 2003.*

[206] Leonard, June 12, 2003, op. cit.

[207] Strohm, Jan. 12, 2005, op. cit.

Security and Governmental Affairs, would require DHS, among other things, to establish best practices for state and local governments in making determinations about the public disclosure and sharing among emergency management personnel of sensitive nonfederal homeland security information and to provide training based on a best practices curriculum. No further action has occurred.

SBU Information in Relation to FOIA

Agencies differ about whether or not SBU information is automatically exempt from disclosure under FOIA. This contentious policy issue has been addressed in existing law, Department of Justice (DOJ)documents, congressional hearings, and in statements issued by the American Bar Association, among others. Contrasting differences in interpretation characterize this issue. As noted, the CSA specified it "was not to be construed to constitute authority to withhold information sought pursuant to the FOIA, or to authorize any federal agency to limit, restrict, regulate, or control, among other actions, the disclosure, use, transfer, or sale of any information disclosable under the FOIA...."[208] According to the DOJ's *Freedom of Information Act Guide*, May 2004, SBU and SHSI are not to be exempt from disclosure under FOIA, except for CII (which is protected pursuant to P.L. 107-296) and other kinds of sensitive information protected by statute — which now includes SSI (pursuant to P.L. 107-296), some land remote sensing geospatial information (pursuant to P.L. 108-375), and some information controlled by the Nuclear Regulatory Commission. As Relyea and Seifert conclude "[i]t seems unlikely, however, that 'sensitive but unclassified' homeland security information, per se, could be protected from disclosure pursuant to the FOIA because it does not appear to fall clearly within any of that statute's exemptions."[209]

Nevertheless, there is ambiguity. For instance, as described above, the DOJ *Freedom of Information Act Guide* describes broad court interpretations that may permit justifiable withholding of sensitive information under FOIA.[210] Also, the

---

[208] 101 Stat. 1730: 40 U.S.C. paragraph 759 note, subsequently repealed in 1996, 110 Stat. 680, As cited in Relyea and Seifert, op. cit., p. 19.

[209] Relyea and Seifert, op. cit., p. 20.

[210] According to the DOJ *Freedom of Information Act Guide*, May 2004, SHSI and SBU are not automatically to be classified pursuant to Executive Order 12958 and "[t]erms such as 'SHSI' and 'SBU' describe broad types of potentially sensitive information that might not even fall within any of the FOIA exemptions...." See the discussion on exemption one. Furthermore, use of these labels does not provide protection from disclosure under any exemption. When discussing exemption two, the *Guide* reviewed the ability to withhold CII data under exception 3 and exemption 2's protections for such homeland security-related information as agency vulnerability assessments and evacuations of CII. It noted that "[s]ince September 11, 2001, all courts that have considered nonclassified but nonetheless highly sensitive information, such as container-inspection data from a particular port ... or maps of the downstream flooding consequences of dam failure ... have justifiably determined — either under exception 2, or, upon a finding of a law enforcement connection ... under exemptions 7 (e) or 7 (f) — that such information must be protected from disclosure....." The same discussion noted that under exemption two, agency officials

(continued...)

Administration has issued instructions to agencies to attempt to use FOIA to protect information if release would harm homeland security. The Card memo, discussed earlier and which guides agencies on handling of SBU information, referred to the Attorney General's memo of October 2001, which instructed agencies, when making discretionary decisions to determine if information is exempt from disclosure under a FOIA exemption, to withhold information if it is legal to do so. It emphasized that agencies should to try to withhold sensitive information under FOIA to protect the nation from terrorist threat, and said that the Department of Justice would support agency determinations.

Agencies also differ on how requests to release information under FOIA will be handled. Illustrations of the variety in federal agencies' proposed or existing policies are given in **Appendix A** and are outlined here. The Nuclear Regulatory Commission (NRC) issued proposed rules in February 2005 for "Safeguards Information" (SGI) — unclassified sensitive information deemed too sensitive for public release, which it said should be withheld from public access and released only to those with a "need to know" even though it was not classified.[211] In 2005 guidance, CDC said its SBU information is information that is exempt from disclosure under FOIA.[212] This was modified in 2006 to require that if a request is received for a document marked SBU, it should be reviewed to determine if it qualifies for an exemption under FOIA and withholding.[213] DHS's management directive 11042.1 on SBU said all information identified as SBU should be labeled FOUO and would include any information that might adversely affect the national interest or the conduct of federal programs; information so labeled and requested under FOIA would be released only on a case-by-case basis, will not be distributed to unauthorized persons, and should be protected and disseminated only to those with a "need to know." The DHS draft directive on categorical exemptions for environmental impact information, dated June 14, 2004, proposed exclusion for disclosure under FOIA. Some parts of DOD automatically exempt SBU information from FOIA. Thus, according to the Defense Security Service, "[t]he term sensitive unclassified information as used here is an informal designation applicable to all those types and forms of information that, by law or regulation, require some form of protection but are outside the formal system for classifying national security information. As a general rule, all such information may be exempt from release to

---

[210] (...continued)
should protect internal agency records that could cause harm.

[211] As authority, it cited section 147 of the Atomic Energy Act of 1954 as amended and specifically, 10 CFR 2.390. For additional information about the NRC process, see **Appendix A** to this report**.**

[212] See **Appendix A** to this report. The source is *Sensitive Information Protection Manual*, attached to a directive. "Sensitive But Unclassifed Information," Manual Guide-Information Security CDC-02, July 22, 2005, not paginated, see about p.3, 8, 10. First reported in "CDC Issues Policy on Sensitive But Unclassified Info," *Secrecy News,* Aug. 2, 2005.

[213] CDC, *Sensitive But Unclassified*, February 2006, as posted at [http://www.fas.org/sgp/othergov/cdc-sbu-2006.html], by Steven Aftergood, *Secrecy News*, Feb. 27, 2006.

the public under the Freedom of Information Act."[214] Other parts of DOD use the FOUO designation only for documents already exempt from FOIA.[215]

DOE equates SBU and OUO, requiring that information be exempt under one of FOIA exemptions two through nine, and exempts all SBU information, which it calls OUO, from disclosure under FOIA, except that it says it will be made available to those with a "need to know" for their jobs.[216] The Federal Energy Regulatory Commission (FERC) issued a final rule outlining access procedures to critical energy infrastructure information (CEII), an SBU category it uses only for information that is exempt from disclosure under FOIA but that it makes available to those with a "need to know." A congressional witness criticized this policy:

> The most glaring problem with FERC's policy is that it is based on the assumption that this information is exempt from disclosure under FOIA. However, FERC's claims are based not on any court-accepted interpretation of FOIA, but on the Justice Department's potpourri of possible exemptions. ...The other problem is that FERC wanted to continued to share this information during its proceedings, requiring it to create a non-FOIA process of disclosure to those parties with a 'need to know,' which required parties to sign a nondisclosure agreement. It is difficult to see how information that was previously public could become non-public based solely on agency regulations.[217]

Reportedly in 2006, controversy arose between Connecticut's State Attorney General and FERC about the state's attempt to access information regarding a proposed Liquified Natural Gas (LNG) plant. The state sought information to review design and safety considerations and to determine whether building the plant would endanger the health and safety of state residents. Reportedly, FERC says the information is not publicly releasable because it is critical energy infrastructure information (CEII), a category of "sensitive but unclassifed," which it says is not releasable under FOIA.[218]

According to the USDA, its SBU information, some of which it calls SSI information, is releasable under FOIA, but that it will process FOIA requests in accord with the instructions in the Attorney General's 2001 memo which instructs

---

[214] Defense Security Service, Employees Guide to Security Responsibilities, "Protecting Sensitive Unclassified Information," [http://www.dss.mil/search-dir/training/csg/security/S2unclas/Intro.htm].

[215] "Background on Sensitive But Unclassified Information," *OMB Watch,* [http://www.ombwatch.org/article/archive/238?TopicID=2].

[216] See **Appendix A**. Source: DOE, "Commission on Science and Security in the 21st Century, DOE accompanied by Recommendations, June 20, 2002. The statement referenced a DOE document *Subject: Identifying and Protecting Official Use Only Information,* DOE Order M 471.3-1, Apr. 9, 2003 (which is current through Apr.2007).

[217] Testimony by Harry Hammitt before the House Subcommittee on National Security, Emerging Threats and international Relations, Mar. 2, 2005, p. 7.

[218] "Sensitive But Unclassified Info: You Can't Have It. Why? Because They Say So." *OMB Watch,* Feb. 22, 2006.

agencies to protect the release of sensitive information under FOIA and to be cognizant especially of exemptions two, three, four and seven.[219]

As indicated above, some agencies require a form of clearance for persons to see SBU information or a determination that they have a "need to know," which could imply exemption from public disclosure.[220] Thomas S. Blanton, Director of the George Washington University National Security Archive, testified at the March 2, 2005 hearing that use of the term SBU thwarts the intent of FOIA and almost forces government bureaucrats to withhold such information:

> We have heard from officials at the Department of Justice that these new pseudo classifications are simply guidance for safeguarding information, and do not change the standards under the Freedom of Information Act. But such a claim turns out to be mere semantics: In every case, the new secrecy stamps tell government bureaucrats "don't risk it"; in every case, the new labels signal "find a reason to withhold." In another TSA response to an Archive FOIA request, the agency released a document labeled "Sensitive But Unclassified" across the top, and completely blacked out the full text, including the section labeled "background" - which by definition should have segregable factual information in it. The document briefed Homeland Security Secretary Tom Ridge on an upcoming meeting with the Pakistani Foreign Minister, but evidently officials could not identify any national security harm from release of the briefing, and fell back on the new tools of SBU, together with the much-abused "deliberative process" exemption to the Freedom of Information Act.[221]

Actions, Including Congressional Action, to Clarify FOIA, with Implications for SBU. On February 13, 2006, the American Bar Association House of Delegates adopted a recommendation, accompanied by a background report,[222] that "urges the Attorney General of the United States to issue a memorandum to Freedom of Information Act (FOIA) officials at federal agencies clarifying that the designation of agency records as 'sensitive but unclassified' cannot be a basis for withholding agency documents from release." The recommendation also called for establishing a standard policy for " ... designating information as "sensitive but unclassified; ... the internal handling of such information; ...taking into account the sensitive nature of such information; and ... ensuring the release of such information unless exempt under FOIA."

Legislative action has been taken to clarify the relationship of some SBU information to FOIA. For instance, as noted above, in 2004, Congress tightened controls on some geospatial information by creating a new FOIA exemption three category to permit the withholding of some land remote sensing data (Sec. 914 of P.L. 108-375). In contrast, during the 109th Congress, H.R. 426, reported out of committee on June 27, 2005, would expand the applicability and use of remote

---

[219] See **Appendix A.**

[220] See **Appendix A**.

[221] Available at [http://www.gwu.edu/~nsarchiv/news/20050302/index.htm].

[222] Available at [http://www.fas.org/sgp/news/2006/02/aba-sbu.pdf].

sensing and other geospatial information to address state, local, regional, and tribal agency needs.

Additional legislation related to these subjects in the 109th Congress includes S. 622, the "Restoration of Freedom of Information Act of 2005." It would amend P.L. 107-296, the Homeland Security Act of 2002, by limiting voluntarily submitted critical infrastructure information provisions in the law that create new exemptions from FOIA; by modifying the FOIA exemption to information submitted as CII records to prevent all CII information submitted by industry from being categorized broadly as an agency record subject to withholding under FOIA; by allowing records to be shared within and between government agencies; by decriminalizing actions of legitimate whistleblowers who might use such information; and by not restricting congressional use or disclosure of voluntarily submitted critical infrastructure information. No action has been taken on the bill, which was referred to the Committee on the Judiciary.

Senator John Cornyn, Chairman of the Senate Judiciary Subcommittee on the Constitution, Civil Rights, and Property Rights, addressing the alleged lack of oversight of FOIA and possible over-classification and over-withholding of federal information, said he planned to hold oversight hearings in the 109th Congress to examine updates that might be needed in the FOIA law to continue to provide citizens with access to government information.[223] The Senate Judiciary Committee's Subcommittee on Terrorism, Technology, and Homeland Security held a hearing on March 15, 2005 on this topic and on S. 394, the "Openness in Government and Freedom of Information: Examining the Open Government Act of 2005." Among other things, the bill would amend FOIA with respect to oversight of requests for information and release of it. A related house bill is H.R. 867. No further action has occurred.

S. 589, the "Faster FOIA Act of 2005," would strengthen FOIA by creating an advisory commission tasked with proposing ways to reduce delays in responding to FOIA requests and would ensure the efficient and equitable administration of FOIA throughout the federal government. It was reported favorably without written report and approved by the Senate Judiciary Committee on March 17, 2005. The House companion, H.R. 1620 was referred to the House Committee on Government Operations. No further action has occurred in the House or the Senate.

S. 1181 requires that any future legislation to establish a new exemption to FOIA must be stated explicitly within the text of the bill. Specifically, any future attempt to create a new so-called "(b)(3) exemption" to FOIA must specifically cite that section of FOIA. The bill sets congressional intent that documents should be available to the public under FOIA unless Congress explicitly creates an exception. It would prohibit applying the FOIA to matters specifically exempted from disclosure by a statute (other than open meetings under the Government in the Sunshine Act) enacted after July 1, 2005, that specifically cite this Act and either: (1) requires that

---

[223] John Cornyn, "Ensuring the Consent of the Governed: America's Commitment to Freedoms of Information and Openness in Government," *LBJ Journal of Public Affairs*, Fall 2004, pp. 7-10.

the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (2) establishes particular criteria for withholding or refers to particular types of matters to be withheld. The Senate approved the bill on June 24, 2005; subsequently, it was referred to the House Committee on Government Reform.

S. 1873, the "Biodefense and Pandemic Vaccine and Drug Development Act of 2005," introduced in the 109th Congress, would "prepare and strengthen the biodefenses of the United States against deliberate, accidental, and natural outbreaks of illness" and would establish a new Biomedical Advanced Research and Development Agency (BARDA), whose activities and information would be categorically exempt from disclosure under the Freedom of Information Act (FOIA). The bill was reported amended without written report by the Senate Committee on Health, Education, Labor, and Pensions, on October 25. It now awaits action by the full Senate. There has been opposition to such blanket exemption because reportedly, no other federal agency has such universal exemption from FOIA.[224]

Federal Information Systems and Automated Identification Processes Used for Sensitive Information

Recognition of federal agency use of the category SBU is illustrated by the need, often mentioned in GAO reports, for agencies to share sensitive information especially relating to homeland security,[225] and the fact that agencies are developing implementation policies and information systems to control and transmit this category of information among those with a need to know it. In addition, some agencies have begun to develop encrypted or protected federal information systems to transmit SBU information to persons who have received approval from an originator or other form of clearance to use them, including first responders, who usually need to sign nondisclosure statements and could be punished for violations of transmittal to third parties. (For additional information, see **Appendix B** on "Illustrations of Federal Information Systems Created to Transmit Sensitive But Unclassified Information Systems.")[226]

In addition, some agencies are using visualization analysis or other automated processes to identify and control sensitive information. For instance, the Idaho National Laboratory, sponsored by DOE in cooperation with Pacific Northwest National Laboratory, reportedly has developed an automated system, a software program called Mozart, that automates identification of sensitive information on a

---

[224] Eugene Russo, "Biodefense Bill Flawed, Says American Society For Microbiology, Other Critics," *Research Policy Alert,* Nov. 9, 2005; "Senate Bill Would Increase Biodefense Secrecy," at [http://www.fas.org/irp/congress/2005_cr/s1873.html], [http://pogoblog.typepad.com/pogo/2005/10/bioshielding_in.html], and [http://www.armscontrolcenter.org/archives/002155.php].

[225] See, for instance, GAO, *High-Risk Series, An Update,* Jan. 2005, GAO-05-207, pp. 15-20, which addresses why the federal government needs to share homeland security information and to standardize policies. See also Tim Starks and Zack Phillips, "Washington and Critical Industries Still Feeling Their Way Toward a System to Share Security Data," *CQHomeland Security,* Dec. 14, 2004.

[226] See also CRS Report RL32597, op. cit.

website by "...using advanced intelligence analysis algorithms, [and] provides a report that can be used to determine if there is sufficient information on a site's Internet web pages to compromise sensitive, proprietary, or classified activities or support adversarial targeting of individuals and programs."[227] As another example, the Department of Energy contracted with a research group at the University of Nevada, Las Vegas, to develop and install on 3,000 computers a program called the "Homeland Security Classifier." It reads and sorts electronic text documents "by applying the same rules used by human classifiers" to identify sensitive nonclassified information, or to categorize a document as releasable.[228]

Inconsistency in Agencies' Processes To Identify SBU Information

Federal agencies use a variety of different concepts of SBU information and methods to restrict public access to it. Labels include such terms as FOUO, SSI, SHSI, CEII, OUO, "limited official use" (LOU), "law enforcement sensitive," and "controlled unclassified information." A CDC manual identifies at least 14 such labels that federal agencies use, and other inventories contain 50 or more such categories.[229]

As illustrated by the descriptions in **Appendix A,** while some agencies use the FISMA-mandated processes to categorize information and implement information security protections based on the level of risk associated with unauthorized access, some agencies continue to use a definition of "sensitive" that is based on the CSA definition, which leads to identification and implementation policies that are based on type or content of information or threat. For instance, the Department of Homeland Security, in its SBU management directive 11042.1, included the Computer Security Act and its definition of "sensitive" as the first item under the heading "Policy and Procedures" that govern the directive, but said " ... with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as

---

[227] Greg Griffin, "Program Management Perspective: Sensitive Unclassified Information," *The Dragon's Breath,* April 2003. See also [http://wwww.pnl.gov/isrc/mozart.faq.html]. See also, a document issued by the Pacific Northwest National Laboratory, a Department of Energy affiliated national laboratory, in "F.A.Q. Mozart," at [http://www.pnl.gov/isrc/mozart/faq.html].

[228] Cate Weeks, "Finding Needles in the Haystack," *UNLV Magazine,* Summer 2004.

[229] *Sensitive Information Protection Manual*, attached to the directive. "Sensitive But Unclassified Information," Manual Guide-Information Security CDC-02, as first reported in "CDC Issues Policy on Sensitive But Unclassified Info," Secrecy News, Aug. 2, 2005. A private group identified about 50 such categories. See, *Secrecy Report Card 2005, Quantitative Indicators of Secrecy in the Federal Government*, op. cit., pp. 9-10. See also Sara E. Kelley, "A Selected Bibliography on 'Sensitive But Unclassified' and Similarly Designated Information Held by the Federal Government," Dec. 17, 2005, at [http://www.llrx.com/features/sbu.htm]. Another author says there is evidence of the federal use of over 60 federal SBU terms: Laura Gordon-Murnane, "Shhh!!: Keeping Current on Government Secrecy, *Searcher*, Jan. 2006.

'sensitive information' does not exist within the federal Government. Such designations are left to the discretion of each individual agency."[230]

The OMB still refers to the concept of "sensitive" as it appears in the CSA in its guidance for information security, Appendix III, "Security of Federal Automated Information Resources," of OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, which is dated November 28, 2000, but is identified on the OMB website as the current circular.[231] It says that "[t]he Appendix ... incorporates requirements of the Computer Security Act of 1987 ... and responsibilities assigned in applicable national security directives." This circular may be confusing because, while it acknowledges the need for agencies to use broader NIST risk-based procedures and guidance to provide information security for all information,[232] it does not mention the FISMA Act or the specific concepts it embodied. The Appendix continues, at times, to refer to the narrower CSA concept of sensitive information that was rendered moot with passage of FISMA. For instance, it continues to refer to the CSA's requirements for agencies to protect computer systems containing sensitive information, and for the Secretary of Commerce to "develop and issue appropriate standards and guidances for the security of sensitive information in federal computer systems."[233]

In a somewhat obscure document — a "note" of July 3, 2003 — the OMB gave specific guidance to agency Chief Information Officers to use FISMA processes.[234] The attached sheets, entitled "Certification and Accreditation — What An Agency Can Do Now," refer to FISMA and certain pertinent NIST publications and say "The need for determining the sensitivity of the information (risk level) as it relates to high, medium, and low needs for the confidentiality, integrity, and availability of the data ... are required in NIST SP 80-18 and must be part of the system security

---

[230] MD 11042.1, op. cit., pp. 3-5.

[231] The appendix establishes "a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123."

[232] The Circular says, "The focus of [previous bulletins] was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information, and focuses extra security controls on a limited number of particularly high-risk or major applications"(Section B. Descriptive information). On the same page it says "The Computer Security Act requires that security plans be developed for all federal computer systems that contain sensitive information. Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality, and therefore all systems require security plans."

[233] Appendix III to OMB Circular A-130.

[234] "Note to Agency Chief Information Officers on "Guidance on Certification and Accreditation," from Mark Forman, administrator, OMB Office of E-Government and IT, July 3, 2003.

plan."[235] It also referred agencies to a then forthcoming document, NIST SP 800-37, and other documents that it instructed agencies to use. It admonished that "FISMA requires assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency."[236]

Among other major federal agencies, the Department of the Army and DOD appear to base some major concepts of SBU on the CSA definition of "sensitive" information that is not classified. DHHS clearly appears to use a FISMA-based risk process; USDA uses a mixed FISMA and CSA approach; agencies that use their own definitions include DOE, NRC, DOD, NRC, and FERC. (For an illustration of the definitions and procedures agencies use to define SBU information and processes to control it, see **Appendix A**, "Illustrations of Federal Agency Controls on Sensitive Information.")

Activities Relating To Developing a Standard Definition of SBU Information

Critics have often decried the proliferation of SBU concepts and the resulting differences in implementation policies — which make it difficult for researchers, agency staff who label and protect information, and public users to know what information is, or is to be, labeled SBU. For instance, Representative Henry A. Waxman, ranking Minority Member of the House Committee on Government Reform, in a March 1, 2005 letter to the Chairman of the Committee's Subcommittee on National Security, Emerging Threats, and International Relations, criticized the increasing proliferation of "pseudoclassification" categories like SBU and the fact that not all documents marked SBU would be legitimate threats to national security if released.[237] During a hearing held on March 2, 2005, on "Emerging Threats: Overclassification and Pseudoclassification," he remarked that the term SBU was used inappropriately to withhold information from the public who need to know it or to prevent the public from seeing inaccurate or politically embarrassing documents.[238] The DHS, he contended, used the SBU designation to withhold the identity of the ombudsman that the public is supposed to contact about airline complaints.[239] Mr. Waxman concluded in his letter to the chairman, which was made part of the hearing record, that "... the executive branch is creating new categories of 'sensitive but unclassified' information that ... lack a statutory basis, and there is no

---

[235] Attachment to Note, July 3, 2003, op. cit., p.2.

[236] Attachment to Note, July 3, 2003, op. cit., p. 3.

[237] Rep. Henry Waxman letter to Hon. Christopher Shays, Chairman of the Subcommittee, Mar. 1, 2005. See also Rebecca Carr, "Government Secrecy Grows With Use of New Stamps," *The Oxford Press News,* Mar. 3, 2005.

[238] Testimony of Rep. Henry Waxman, *Emerging Threats: Overclassification and Pseudo-Classification,* Hearing before the Subcommittee on National Security, Emerging Threats, and International Relations of the House Committee on Government Reform, Mar. 2, 2005, 109th Congress, lst session.

[239] Waxman, testimony, Mar. 2, 2005, op. cit.

federal entity monitoring their use."[240] Another witness at the March 2005 hearing testified that "[t]hese ill-defined categories — be they 'sensitive but unclassified,' 'sensitive security information,' or some form of 'critical infrastructure information' — almost always do more harm than good. They ... are based on ... an antithetical proposition in our democracy — that, when in doubt, always favor secrecy over openness."[241]

Dr. Ron Ross, a principal author of NIST's security standards mandated by FISMA, commented that there are

> dozens of different definitions of "sensitive unclassified information" across the federal government. Originators, or information owners, have discretion in identifying, marking, controlling, protecting, and releasing sensitive unclassified information resulting in: uneven and inconsistent protection of information assets; varying degrees of risk resulting from different release criteria; and inability to share information across organizational boundaries with confidence and trust.[242]

William J. Leonard, the director of the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA), which conducts periodic inspections and reviews classification and declassification plans, criticized the "... lack of common understanding of what exactly sensitive information is, how to identify it, and how and when to protect it."[243] He emphasized that the federal government needs a reasonable policy to share or withhold information and "in many instances, 'sensitive but unclassified' is a label without meaning that is misused by officials who lack the proper 'training, background or understanding' to decide what to withhold."[244] He is reported to have said "The DHS policy 'creates an environment exactly opposite ... [from] what we're trying to do in the name of information sharing.... It creates an environment of uncertainty.'"[245] Workers in government agencies are confronted with a proliferation of many SBU protection "regimes" and "... will prefer to err on the side of caution, or withholding

---

[240] Waxman, letter to Hon. Christopher Shays, Mar. 1, 2005, op. cit., p. 12.

[241] According to testimony by Harry Hammitt before the House Subcommittee on National Security, Emerging Threats, and International Relations, Mar. 2, 2005, p. 8.

[242] Ron Ross, "Protecting Controlled Unclassified Information, A Strategy for Effectively Applying the Provisions of FISMA, Presentation to the Joint Futures Laboratory," [2005], p. 11.

[243] William J. Leonard, "Speech to Classification Managers," June 2004, "Challenges to Information Sharing and Protections Post 9/11," In *Special Report: Government Security Panel Report* at [http://www.cip.umd.edu/special/govsecpanel_report_29july04.htm].

[244] R. Jeffrey Smith, May 29, 2004, op. cit.

[245] "DHS Non-Disclosure Agreements Stir Concern," *Secrecy News*, Dec. 6, 2004, citing Eileen Sullivan, "Searches and Gag Orders: Homeland Security's Unprecedented Campaign Cloaks Unclassified Info," *Federal Times*, Dec. 6, 2004. See also "Homeland Secrecy," *Washington Post*, Dec. 3, 2004, p. A26.

information, out of confusion and/or a fear of getting in trouble."[246] According to Leonard,

> ... a water works operator may submit a report of anomalous activity involving the water authority. Standing by itself, that information may appear innocuous; however, it may be a critical link, for example, to a public health official dealing with his or her own anomaly. That public health official should be able to access and become aware of that information from the waterworks operator without a supposedly omniscient authority in the middle making singular decisions as to who should receive the information and who should not. The essence of information sharing is that the entity on the "edge" should be in a position to receive the same information as those at the "center.[247]

He wrote that consistent standards require a common lexicon, a common governmental authority responsible to "revalidate and synchronize the various existing regimes controlling unclassified information,"[248] and "... a simplified framework that can serve as a template for the identification, control and protection of unclassified information whose dissemination is controlled." Among its potential benefits, such a framework would have "great specificity with respect to what information is covered and what is not covered [and] limits on who could designate information as controlled. It would allow discretion to not use controls "even if the information is eligible." It would have "[b]uilt-in criteria that must be satisfied in order to place controls on dissemination," recognize due-diligence standards about handling and protecting information, a fixed time duration for control, and an appeal process."[249]

As noted above, the ABA House of Delegates adopted a resolution on February 13, 2006, that among other things called for establishment of a standard policy to designate, handle, and release such information except if it is exempt under FOIA.

Recognition of the need for basic standardization of homeland security-related, sensitive, unclassified information was made by Congress when it enacted section 892 of P.L. 107-296, which mandated presidential issuance of guidance to define procedures to protect sensitive but unclassified homeland security information. Guidelines have not been issued as of February 15, 2006. Also, as already noted in this report, in December 2005, the President issued instructions to federal agencies to inventory all their SBU information, the authorities invoked to label it SBU, and practices used to protect it, with the objective of generating uniform government-wide standards and procedures for designating, marking, and handling SBU

---

[246] "Challenges to Information Sharing and Protections Post 9/11," In *Special Report: Government Security Panel Report* at [http://www.cip.umd.edu/special/govsecpanel_report_29july04.htm]. (J. William Leonard, Statement.)

[247] "Information Sharing and Protection: A Seamless Framework or Patchwork Quilt?" Remarks at the National Classification Management Society's Annual Training Seminar, June 12, 2003, available at the website of U.S. National Archives and Records Administration.

[248] Leonard, June 12, 2003, op. cit.

[249] Leonard, June 12, 2003, op. cit.

information. In addition, Congress has already addressed certain aspects of how to define SBU information, and additional proposals are under consideration.

GAO Study on SSI. During the 108th Congress, responding to a request by Representative David Obey and Representative Martin Olav Sabo, the GAO assessed the DHS's use of the concept of sensitive security information (SSI) — specifically the procedures to categorize information as SSI, procedures to remove the SSI label, review procedures to check the appropriateness of the SSI designation; and organizational functions relating to taking SSI actions.[250] The Members of Congress were concerned about why information that had already been released to the public, or seemingly nonsensitive information such as government telephone directories, was given the label SSI and about how the TSA distinguished between information that needs to be protected and information the public needs for its own safety. According to Congressman Sabo, "GAO found that TSA has no internal control procedures for SSI designation, and that potentially every TSA employee can stamp something 'SSI.'"[251] The final report was issued as *Transportation Security Administration: Clear Policies and Oversight Need for Designation of Sensitive Security Information,* GAO-05-677, June 2005.

P.L. 109-90 Requires DHS To Improve Use of SSI Categories and Report to Congress. In 2005, Congress enacted legislation, based on language originating in the House and offered by Mr. Sabo as an amendment to the DHS FY2006 appropriations bill, "to clarify 'SSI' policy and procedures including which staff may appropriately have designation authority." According to the Conference Report, House Report 109-241, "... because of insufficient management controls, information that should be in the public domain may be unnecessarily withheld from public scrutiny...."[252] Section 537 on "Sensitive Security Information" of the enactment, P.L. 109-90, requires the DHS Secretary to ensure that there is an official within each appropriate office with clear authority to "designate documents as SSI and to provide clear guidance as to what is SSI material and what is not." It noted that a limited number of appointed officials pursuant to 49 CFR 1520.5(b(1)-(16)) have authority to designate such information. Section 537 also required the Secretary to report to the Appropriations "... Committees not later than December 31, 2005 on "(1) Department-wide policies for designating, coordinating and marking documents as SSI; (2) Department-wide auditing and accountability procedures for documents designated and marked as SSI; (3) the total number of SSI coordinators within the Department; and (4) the total number of staff authorized to designate SSI documents within the Department." According to DHS staff and committee staff, this report has

---

[250] "Audit of Sensitive Security Information Requested," *OMB Watch,* Sept. 21, 2004, [http://www.ombwatch.org/article/articleprint/2409/-1/83]. See also Steven Aftergood, *Secrecy News,* June 11, 2004 and Sept. 23, 2004.

[251] Office of Rep. Sabo, "Sabo Amendment Addresses Abuse of 'SSI' Designation Within the DHS," press release, May 10, 2005.

[252] U.S. Congress. Committee of Conference. *Making Appropriations for the Department of Homeland Security for the Fiscal Year Ending September 30, 2006, and for Other Purposes*, 109th Congress, lst sess., [On H.R. 2360], House Report 109-241, Sept. 2005, p. 37.

been sent to the committees, but may need to be modified.[253] Also, by January 31, 2005, the Secretary of Homeland Security is to report to the Appropriations committees the titles of all documents that were designated by DHS as SSI in their entirety between October 1, 2005 and December 31, 2005, and for each year thereafter. According to DHS staff, this report has been prepared and was transmitted to the committee.. The Secretary is also charged with providing examples of DHS guidance on designation of the 16 SSI markings that will "serve as the primary basis and authority for the marking of DHS information as SSI by covered persons" (Sec. 537).

Legislation Introduced on "Pseudo-Classification". H.R. 2331, the "Restore Open Government Act of 2005," was introduced in the 109th Congress. It is similar to H.R. 5073 of the 108th Congress and called for an end to the use of SBU and FOUO and related terms[254] without defining them. Among other things, it would revoke the Ashcroft and the Card memos released in 2001 and would seek to curtail excessive classification. It would direct the Archivist of the United States to (1) report on the use of pseudo-classification designations; and (2) promulgate regulations banning unnecessary pseudo-classification designations and standards for withholding nonclassified information. It would restore presumption of disclosure under FOIA, facilitate public access to critical infrastructure information, address alleged excessive over-classification, and make it easier to challenge agencies that are accused of improperly withholding information. The bill was referred to two committees, House Government Reform and House Homeland Security. No action has been taken on the bill.

GAO Study on SBU. The GAO is inventorying and reviewing selected federal agencies' policies and procedures relating to the handling of SBU information in response to requests made by Representative Tom Davis, Chairman, House Committee on Government Reform; Representative Todd Platt, Chairman, House Committee on Government Reform, Subcommittee on Government Management, Finance and Accountability; Representative Christopher Shays, House Committee on Government Reform, Subcommittee on National Security, Emerging Threats, and International Relations; and Senator Susan Collins, Chairman, Senate Committee on Homeland Security and Governmental Affairs. The study will look at agency use of such information control terms as SBU, FOUO, LOU, law defense controlled unclassified information, and others. The report is expected to be finished in March 2006.[255]

---

[253] Interview with DHS and committee staff members, February 2006 and March 2006.

[254] According to section 5 of the bill, "'pseudo-classification designations' means information control designations, including 'sensitive but unclassified' and 'for official use only,' that are not defined by Federal statute, or by an Executive order relating to the classification of national security information, but that are used to manage, direct, or route Government information, or control the accessibility of Government information, regardless of its form or format."

[255] Identified in the GAO system as "Major Challenges Related to Information Sharing," study number 310483.

Option To Monitor Agency Use of Risk-based Standards for Sensitive Unclassified Information

As noted above, some agencies appear not to have implemented procedures as prescribed in FISMA to protect information, including sensitive information, with controls based on risk of release. Some may ask, why have they not done so? Agencies may not know that the CSA "sensitive information" definition was rendered moot, especially because major agencies, including OMB and DHS, still reference CSA and use the term in various documents and guidances. The CSA definition may be easy to use since it is broad and has been used for almost 20 years. It is possible that some agencies may not be fully aware that the E-Government Act extends to handling of all types of information, including what they categorize as SBU or sensitive information. Slow compliance with the FISMA guidance may also be due to the fact that NIST has not yet formally released the final volume in its FIPS series — the volume cataloguing actions agencies can take to protect information at various levels of risk. However, the preceding volumes, which give agencies guidance on procedures to use to define information types and risk levels, have all been released. Also, according to GAO, Inspector General reports, and testimony in various congressional hearings, many agencies have not yet formally incorporated an overall risk management program into their information security policies because they are slow to implement the legislative mandates or are finding it too expensive to comply with the mandates of the E-Government Act.[256]

Some information handlers may be wary of the NIST processes because they believe that risk-based standards prescribed by NIST are too loose for their circumstances, the threats, and the potentially malevolent uses of information confronting their agency. They may believe that the use of such standards would permit the release of sensitive information that should be protected or that risk-based analysis may not be rigorous enough.[257] Also, agencies may be aware of NIST risk-based standards, but may choose to use other procedures since the law allows agencies to use more stringent procedures to protect information if, in their determination, agencies recognize the NIST standards as mandatory minium standards.

Despite the fact that OMB does not require formal, detailed risk analyses to be conducted, some agencies may not be eager to comply with FISMA, because they might believe that risk-based analyses might be expensive to conduct, or might lead to categorizing a lot of information (whose impact levels might be mixed for the three categories of confidentiality, accessability, and integrity) at the highest level of impact or risk (for any one of the three impacts). Although this might lessen the cost

---

[256] FISMA is Title III of the E-Government Act. See Benton Ives-Halperin, "Effectiveness of Cybersecurity Law Questioned," *CQ Homeland Security,* Nov. 15, 2005.

[257] For a discussion of the purported limitations with respect to computer security, see Benton Halperin, "Risk-Based Analysis Might Not Work in Electronic World, Experts Say," *CQ Homeland Security,* Nov. 23, 2005.

of protection (or raise it), it might also require protecting some information which does not need to be safeguarded at such a stringent level.[258]

Two oversight issues are suggested by these observations. One is to monitor federal agency compliance with FISMA, especially the use of NIST-generated, risk-based standards and information protection procedures to identify and protect all information, including sensitive unclassified information. Another is that in light of the potential confusion resulting from the language of Appendix III to OMB Circular A-130 regarding the basis of agency information security responsibilities, Congress may seek to oversee updating of the appendix document.

Recommendations to Institute Better Governance of SBU Information Procedures

A number of recommendations have been made relating to improving procedures used to administer SBU controls. It is possible that some of these issues may be addressed by the executive branch pursuant to the President's memo of December 16, 2005.

Limit the Number of Persons Who Can Designate SBU. As noted above, especially in the comments of ISSO Director Leonard and others, many governmental officials can stamp a document SBU. It was reported that although a limited number of government personnel (estimated at more than 4,000)[259] can stamp classified documents "top secret" (which can be declassified after review according to a regular schedule, or whose classification can be appealed), many more employees can stamp documents SBU (whose designation is not on a schedule to be reviewed or changed and for which there are no appeal process.) Specific comments in this regard were made about DHS's SBU policies:

> the new FOUO information policy is actually more far-reaching than national security classification policy. Thus, classified information can only be generated by officials who have been authorized by the President, either directly or indirectly by delegation. But any DHS employee or contractor can designate information a FOUO if it falls within eleven broad categories. Moreover, managers and supervisors can also designate additional information as FOUO even if it falls outside of those categories. Further, the classification system provide for an oversight mechanisms through the Information Security Oversight Office. No provision for oversight of the new FOUO policy is included.[260]

One option for policymakers may be to consider limiting the number of persons who can designate information as SBU. This option might have other consequences. It could force agencies to develop formal systems to categorize SBU information, with

---

[258] Conversation with Ron Ross, NIST, Feb. 2005.

[259] Paul McMasters, "Your Right to Know," *Star — Telegram.com,* Mar. 13, 2005.

[260] "Dept of Homeland Security Tightens Grip on Unclassified Info," *Secrecy News*, June 11, 2004). See also comments of Aftergood and others in "Challenges to Information Sharing and Protections Post 9/11," In *Special Report: Government Security Panel Report*, [http://www.cip.umd.edu/special/govsecpanel_report_29july04.htm].

the designation responsibility limited to a few selected individuals, similar to national security information "classification" procedures. Such a development could also legitimize SBU designation as a formal classification category and cause added expense to agencies.

Options To Centralize Policy Control for SBU Information. The President's December 16, 2005 memo appears to have centralized the development of SBU policies in the Director of National Intelligence (DNI), who is to develop policy "in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General and in consultation with all others heads of relevant executive departments and agencies...."[261] Control by the DNI may imply the development of SBU information control policies that may be more restrictive than some critics would prefer.[262]

There are also proposals to establish a central authority elsewhere in the federal government to develop policy and guidelines for SBU information — such as in OMB, the NARA's Information Security Oversight Office (ISOO), the Interagency Security Classification Appeals Panel (ISCAP), or within the judicial system. For instance, a report released in December 2004 by the Heritage Foundation and the Center for Strategic and International Studies concluded that centralization, perhaps in OMB, could assist in inventorying which information might be sensitive and in developing standardized policies:

> To date, there has been no systematic review of what government information that is now or was formerly in the public domain could be used as a "terrorist roadmap," the likelihood of such a threat, the role that such information would play in terrorists' preparation (including possibilities of alternative sources of the same information), and the countervailing public safety and other benefits of providing different types of information. Furthermore, no authority is clearly designated to make these evaluations at a national policy level. Current evaluations are conducted at the departmental level at best or on an ad hoc, office by-office basis. Nor has DHS provided any leadership or guidance to the private sector about how the private sector might develop voluntary standards for making decisions about its own disclosures of sensitive information, even without governmental restrictions. For government decisions, there is no single designated authority — in the Office of Management and Budget or elsewhere — for determining the overall policy interests and objectives of information distribution, including common baseline standards to help weigh the benefits and risks of providing the public with specific types of information, regardless of which agencies possess the information. Such a single authority might act as the

---

[261] Guideline 3 of "Guidelines and Requirements in Support of the Information Sharing Environment," Memorandum for the Heads of Executive Departments and Agencies, White House press release, Dec. 16, 2005, op. cit.

[262] While the DNI is to coordinate classified information programs, the function reportedly will include coordinating efficient sharing of information across the government. See Lance Gay, "Government Withholds 'Sensitive-but-Unclassified' Information," *Scripps Howard News Service*, Feb. 2, 2006.

> overall reviewer of agencies' public disclosure policies and their implementation of these policies....[263]

Similarly, Steven Aftergood, editor of *Secrecy News*, was reported to have observed that federal agency actions that declare SBU information exempt from FOIA may need better policy guidance and that [i]t may ultimately require judicial action or congressional intervention to define clearer standards for what may be withheld and what must be disclosed."[264] A 2004 Federation of American Scientists' report concluded that oversight of SBU information designations and policy might benefit from coverage in ISOO or ISCAP. It recommended that

> [t]he President could direct the ISOO to expand its portfolio to encompass such sensitive but unclassified information, though to be effective this would require an infusion of new personnel and resources to an organization that is stretched thin. Similarly, the President could task ISCAP to receive and evaluate challenges to controls that have been imposed on unclassified information, in addition to its current oversight of classified information. To avoid diluting or diverting the efforts of these existing entities, it may be preferable to devise a new organization or interagency panel that can tackle controls on unclassified information, while bolstering the work already being performed on oversight of classified information.[265]

An Appeals Process. The need for an appeals process for SBU information has been stressed by critics who allege that the SBU labeling system is more restrictive than federal national security information classification systems. For instance, in testimony, Hammitt contended that "... remedies to challenge the designation of such information must be made available. Requesters must not be forced to go to court as their only alternative. Instead, a process akin to mandatory declassification review should be instituted." He also argued, "Along these same lines, time limits for protection should be considered and implemented. Sensitive information may well be sensitive for a period of time and lose its sensitivity thereafter. Once information is no longer sensitive it should be made publicly available. [The National Archives usually declassifies most material after 25 years, except for nuclear-related information.]."[266] Gansler and Lucyshyn recommended that the National Archives and Records Administration develop and administer an appeals process to allow individual decisions about release of information on a case-by-case basis.[267]

---

[263] Carafano and Heyman, pp. 20-21.

[264] Joe Fitzgerald and Antonia Badway, "Government Secrecy In the Age of Information,"*Biodefense Quarterly,* Summer 2003, p. 2.

[265] *Flying Blind: The Rise, Fall, and Possible Resurrection of Science Policy Advice in the US*, Federation of American Scientists, 2004, by Henry Kelly, Ivan Oelrich, Steven Aftergood, Benn H. Tannenbaum, pp. 63-64.

[266] Harry Hammitt in testimony before the House Subcommittee on National Security, Emerging Threats and International Relations, Mar. 2, 2005, p. 8-9.

[267] *The Unintended Audience: Balancing Openness and Secrecy,* op. cit., p. iii.

Other Remaining Issues and Unanswered Questions

Policymakers may encounter some remaining unanswered questions. Is communication between the intelligence community and the scientific communities adequate enough to enable researchers to identify information that should be protected to prevent terrorists from gaining knowledge to harm the United States? Do SBU controls constitute another type of classification system? Just how much scientific and technical information is being withheld under various SBU designations and how has such withholding affected the conduct of research and development and the use of scientific and technical information in policymaking? Should special considerations be given to allow access to scientific and technical information, especially that produced by universities, since the academic sector has a unique role as a generator of knowledge as a public good and as a significant "engine" of industrial innovation? Will DHS's SBU controls on "developing technology or current technology" affect information generated by DHS-funded research and development grants and contracts? Can risk-based procedures be used effectively to control access to, and dissemination of, scientific and technical information, and can they effectively balance access and control? Would the use of risk-based procedures generate control procedures different from those used in existing SBU information control systems? What is the cost (administrative and financial) of SBU information control regimes, the actions needed to implement them, and to safeguard SBU information indefinitely? Would there be a significant difference in cost-effectiveness calculations for implementing risk-based analysis procedures versus some of the currently used SBU procedures? Should there be monitoring of the use and effects on scientific communication of governmental and private sector voluntary information control procedures? Who should conduct such monitoring?

The President, the Congress, and the scientific community have initiated steps to answer some of these questions. The ongoing activities — to inventory agency activities, to oversee agency policies and procedures, to clarify terminology, and to develop professional groups' codes of conduct and voluntary control procedures — may foster practices that are compatible with the continuous growth of scientific knowledge and dynamics in the emergence of new threats. Competing stakeholder demands will continue to confront Congress and the executive branch as policies are refined to balance security and access to scientific information.

Appendix A. Illustrations of Federal Agency Controls on Sensitive Information

The following information illustrates how agencies define SBU information and the procedures they use to control it. Because agency policies are difficult to obtain, the information in this section is meant to be illustrative and is limited to what is readily accessible. It divides agency descriptions into four categories: (1) Agencies that use the definition of "sensitive"as found in the Computer Security Act; (2) Agencies that use FISMA guidelines or risk-based procedures to develop information security policies; (3) Agencies that mix use of SBU and FISMA concepts; and (4) Agencies that use unique definitions.

Agencies That Use the Definition of "Sensitive" as Found in the Computer Security Act (CSA)

Some agencies use the CSA definition of sensitive, which identifies information based on its content, not on the risk of release.

Department of Homeland Security (DHS). The Department of Homeland Security in a management directive applicable within the agency, released first in 2004 and then revised in January 2005, cited the CSA, P.L. 100-235, and repeated the law's now rescinded definition of "sensitive information" as the first element of policy guiding the directive. It does not necessarily endorse use of this definition but says that "specific, standard criteria and terminology defining the types of information warranting designation as 'sensitive information' does not exist within the federal government. Such designations are left to the discretion of each individual agency."[268]

Office of Management and Budget (OMB). Appendix III, "Security of Federal Automated Information Resources," of OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources,* which is dated November 28, 2000, but is identified on the OMB website in November 2005 as the current circular, references the CSA, but not the FISMA Act. The appendix establishes "a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123." Its guidance could lead to confusion because while it acknowledges the need to use NIST-generated risk-based procedures to protect all kinds of information (not only sensitive information), it says that "[t]he Appendix ... incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives"[269] It continues to use the term "sensitive" and references CSA's requirements for agencies to protect

---

[268] MD11042.1, p. 3.

[269] Appendix III, "Security of Federal Automated Information Resources," to "OMB Circular A-130, Transmittal Memorandum #4, Management of Federal Information Resources (11/28/2000)," op. cit.

computer systems containing sensitive information and the Secretary of Commerce's responsibilities to promulgate standards to protect sensitive information. Guidance issued to a limited CIO readership makes explicit reference to NIST's post-FISMA responsibilities and for agencies to use mandatory, risk-based security standards issued by NIST.

Department of the Army. The Department of the Army uses the term "Controlled Unclassified Information (CUI) Not Subject to Public Disclosure" as including the "categories of 'for official use only,' 'sensitive but unclassified,' which formerly was called 'limited official use,' 'sea sensitive information,' 'DOD unclassified controlled nuclear information,' and 'sensitive information' as defined in the Computer Security Act of 1987."[270] CUI " ... includes U.S. information that is determined to be exempt from public disclosure in accordance with DOD Directives 5230.25 and 5400.7 or that is subject to export controls in accordance with the International Traffic in Arms Regulation or the Export Administration Regulation." For example:

> These types of information include but are not limited to: patent secrecy data, confidential medical records, inter-and intra-agency memoranda that are deliberative in nature, certain data compiled for law enforcement purposes, data obtained from a company on a confidential basis employee personal data, internal rules and practices of a government agency that, if released would circumvent agency policy and impede the agency in the conduct of its mission; and finally technical controlled unclassified information.[271]

National Security Agency. In a 2003 document that appears to still be active, the National Security Agency used the CSA definition to define the term "sensitive information" as "information, the loss, misuse, or unauthorized access to or modification of, that 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. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy." Expanding this definition, it said "(Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235).)"[272]

Centers for Disease Control and Prevention (CDC). CDC's 2005 policy on SBU information was issued in an information security manual on July 22, 2005.[273] Applicable to all employees and contractors, the manual covers information

---

[270] "Controlled Unclassified Information (CUI)" powerpoint slide show, produced by Department of the Army, nondated, available at [http://www.fas.org/sgp/othergov/dod].

[271] "Controlled Unclassified Information (CUI)" powerpoint slide show, op. cit.,

[272] National Security Agency, Committee on National Security Systems, *National Information Assurance (IA) Glossary, CNSS Instruction No. 4009,* Revised May 2003, pp. 55-56 [http://www.nstissc.gov/Assets/pdf/4009.pdf].

[273] *Sensitive Information Protection Manual*, attached to the directive. "Sensitive But (continued...)

"sensitive enough to require protection from public disclosure — for one or more reasons outlined under the exemptions of the Freedom of Information Act, but may not otherwise be designated as national security information." It identified and defined categories of "sensitive but unclassified" information, including one labeled "Computer Security Act Sensitive Information" which it defined as in the CSA, which it cited as the source. The other categories of information CDC defined as SBU include "Contractor Access Restricted Information," "Controlled Unclassified Information," "DEA Sensitive," "Department of State Sensitive But Unclassified," "DOE Official Use Only," "Export Controlled Information (or material)," "For Official Use Only," "GSA Sensitive But Unclassified Building Information," "Law Enforcement Sensitive," "Operations Security Protected Information," "Privacy Act Protected Information," "Select Agent Sensitive Information," and "Unclassified Controlled Nuclear Information." All CDC information has to be reviewed for security and approved before release; relevant information will be protected and encrypted for electronic transmittal, and some aggregated information may qualify as SBU. Violations of the policy may result in civil or criminal action. Healthcare information and public health data and statistics would not be "potentially sensitive." This policy was modified in 2006 to require that if a request is received for a document marked SBU, it should be reviewed to determine whether it qualifies for an exemption under FOIA and withholding from release.[274]

International Boundary and Water Commission (USIBWC). The U.S. section of the International Boundary and Water Commission between the United States and Mexico issued a directive on July 8, 2005, that establishes a policy of "sensitive information protection." Sensitive information is defined similar to, but more broadly than, the definition used in the CSA as

> unclassified information of a sensitive nature not otherwise categorized by federal statute or regulation and the unauthorized disclosure, loss, or misuse of which could adversely impact on the following; a persons' privacy or welfare; the conduct of federal programs; or the conduct of other programs or operations essential to the national interest.[275]

Among the types of information to be treated as sensitive are information exempt from disclosure under FOIA and the Privacy Act, information technology information, and USIBWC internal security measures, including emergency management plans, physical security plans and reports that disclose facility infrastructure or security vulnerabilities, continuity of operations plans, risk management plans, and accreditation and recertification documentation.[276] Such information is to be released only to those who have a "need to know", protections

---

[273] (...continued)
Unclassifed Information," Manual Guide-Information Security CDC-02, as first reported in "CDC Issues Policy on Sensitive But Unclassified Info," *Secrecy News,* Aug. 2, 2005.

[274] CDC, *Sensitive But Unclassified,* February 2006, posted at [http://www.fas.org/sgp/othergov/cdc-sbu-2006.html], by Steven Aftergood, *Secrecy News,* Feb. 27, 2006.

[275] *Sensitive Information Protection Manual*, p. 1, attached to the directive.

[276] *Manual*, op. cit., p. 3.

are required for storage and transmittal, and penalties are imposed for disclosure, including suspension and removal.

Idaho National Engineering and Environmental Laboratory. The Idaho National Engineering and Environmental Laboratory, funded by the Department of Energy (DOE), said in 2003 that DOE in its 1995 safeguards and security glossary defined "sensitive" substantially similar to the way it is defined in the CSA. It then offered a definition that is broader than the one in the CSA:

> Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or government 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 confidentiality of personal or commercial propriety information provided the U.S. government by its citizens.[277]

Agencies That Use FISMA Guidelines or Risk-Based Procedures To Develop Information Security Policies

Some agencies use clearly identified risk-based or FISMA-derived guidelines to develop information security policies.

Department of Health and Human Services (DHHS). DHHS's policy guidance, entitled *Information Security Program Policy*, December 15, 2004,[278] and its *Information Security Program Handbook*, November 12, 2004, contain policy and implementation plans that appear to conform with the NIST guidance documents. They specify that sensitive information that is not subject to national security controls should be protected by a process that includes risk assessments that incorporate threat and vulnerability analyses and development of security programs according to the level of risk involved. The authorities cited for these actions do not refer specifically to homeland security guidance materials, but instead to FISMA, the Clinger-Cohen Act, the Information Technology Management Reform Act (Division E of P.L. 104-106), and OMB Circular A-130.[279] DHHS said it also incorporates the requirements specified in relevant executive orders, Homeland Security Presidential Directives, NIST Special Publications, and so forth. In the DHHS documents, implementation procedures include background checks for accessibility to sensitive information, nondisclosure agreements, protection and encryption procedures, and so forth. These documents apply to information systems, including hardware, software, and data on them of any sensitivity or classification.[280] Use of these concepts replaces the use of

---

[277] Griffin, Apr. 2003, op. cit.

[278] HHS IRM Policy 2004-002.001.

[279] HHS IRM Policy 2004-002.001, pp. 1, 2.

[280] *Information Security Program: Information Security Program Handbook*, Nov. 12, 2004, (continued...)

the term "sensitive" and of the CSA concepts, which DHHS appears to have halted in 2004.[281]

Military Joint Futures Laboratory. The Military Joint Futures Laboratory of the U.S. Joint Forces Command is conducting a study of implementation of SBU information policies and procedures in military programs. Pursuant to DOD guidance, "All DOD unclassified information must be reviewed before it is released to the public or to foreign governments and international organizations."[282] That which is not released in accordance with national laws, policies, and regulations of the originating country[283] shall be stamped FOUO and access control and protection procedures applied. These kinds of information include, but are not limited to, For Official Use Only, Law Enforcement Sensitive, Sensitive But Unclassified, Limited Official Use Only, and Limited Distribution.[284] According an information security analyst, "controlled unclassified information" (CUI) lacks a clear definition, policy guidance, or central authority to develop and mandate control policies. Only the originator of the information can authorize disclosure or release. He suggests using NIST documents and guidance to identify CUI and to conduct threat and vulnerability analysis for information.[285]

Information Sharing and Analysis Centers (ISAC). ISACs are private organizations that collect, distribute, analyze, and share sensitive information

---

[280] (...continued)
pp. 1, 32, and *Information Security Program: Information Security Program Policy,* Dec. 15, 2004, p. 1.

[281] DHHS still referred to the Computer Security Act in its now superceded 2005 update of its *Automated Information Systems Security Programs Handbook* to note that sensitive unclassified agency information should be given the security-level designation "high sensitivity" (the two lower are "low" and "moderate") and should use the next highest level of "high and national security interests" if the loss of it could adversely affect national security interests. DHHS is also developing a new Automated Information Technology Security Program to "document and evaluate the existence and reliability of the Automated Information System Security Program at selected operating divisions. This program helps to protect information resources in compliance with the Computer Security Act of 1987 and the directives of OMB and the National Institute of Standards and Technology." It used the CSA definition of sensitive in DHHS Automated Information Systems Security Program Handbook, available at [http://wwwoirm.nih.gov/policy/aissp.html#OverviewII]. This handbook was superceded by the 2004 documents identified in the text above. Reference to protection of information resources in compliance with the CSA and use of the term "sensitive" appears to have ceased after last used in *HHS/OG Fiscal Year 2005 Work Plan — Department-wide*, p. 5, [http://oig.hhs.gov/publications/docs/workplan/2005/2005WPDptwd.pdf].

[282] "Information Security Challenge for J9 Marking Controlled Unclassified Information (CUI), [Slide show], by Bob Craig, INFOSEC Policy Analyst Briefing to the Joint Concept Development Pathway, as of Mar. 18, 2005.

[283] Craig, Slides, Mar. 18, 2005.

[284] Appendix 3: "Controlled Unclassified Information," of Interim Information Security Guidance, Apr. 16, 2004, on changes to DOD Regulation 5200.1-R, Jan. 1997.

[285] Interviews of Robert Craig, January and March 2005 and Craig, Slides, Mar. 18, 2005.

regarding threats, vulnerabilities, alerts and best practices to protect national critical infrastructures in fields such as chemistry, electricity, energy, financial services, healthcare, information technology, public transit, surface transportation, telecommunications, and water, physical, and cyber security critical infrastructures.[286] They were established in response to Presidential Directive 63, 1998, which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect U.S. critical infrastructures. The directive was updated by Homeland Security Presidential Directive 7 in 2003.

The ISAC information sharing process developed a categorization scheme for unclassified government data, as well as data originating from ISAC members, "based upon level of sensitivity." Vetting of the data is to address four levels. The most restrictive is "Privileged Information/Restricted Use (Level 3) - Information that should only be distributed to individuals who must act, analyze, or make decisions based on the data. Distribute only to individuals with Level 3 Background check. This should include Government 'Sensitive But Unclassified' information and similar very close-hold information."[287] A level 3 background check "[r]equires 10 years of history immediately prior to the background check. Includes felony checks from all jurisdictions in which subject readied during period. Includes scan of additional databases, and personal interviews. Requires recertification every 3 years."[288]

Agencies That Mix Use of CSA and FISMA Concepts

Agencies that use mixed models of the CSA definition and risk-based guidelines include USDA and a DOE-affiliated agency.

U.S. Department of Agriculture. The Department of Agriculture (USDA) promulgated regulations requiring its constituent agencies to issue criteria and directives to identify "sensitive security information," defined as unclassified information that if publicly disclosed could be expected to have a "harmful impact on the security of person, place, or property." Among the science and technology-related "USDA SSI possibilities" it identified "building vulnerabilities, ... select agent pathogen locations, ... USDA computer infrastructure details, rural development management control review that reveal vulnerabilities, ... the ARS report *Strategic Research Targets to Potential American Livestock and Poultry from Biological Threat Agents, ...* security assessment of USDA Non-BSL-03 laboratories, [and] local pathogen inventories for USDA non-BSL-3 laboratories...."[289] Such information should be identified and protected after an informal "... risk analysis and determination to identify potential threats and appropriate vulnerabilities to SSI in

---

[286] "Vetting and Trust for Communications Among ISACs and Government Entities," *ISAC Council White Paper,* Jan. 31, 2004, pp. 5, 6, 8.

[287] "Vetting and Trust for Communications Among ISACs...," pp. 5-6.

[288] "Vetting and Trust for Communications Among ISACs...," p. 6.

[289] Slide show, "USDA Sensitive Security Information, DR3440-2, April 2004."

their custody." [290] Only those who have a "need to know" are to have access to SSI. Need-to-know determinations are to be made by an authorized holder of SSI who attests that a prospective recipient requires access to perform or assist in a lawful and authorized governmental function. Information designated "SSI" should be protected no longer than 10 years, unless a designating official determines otherwise. SSI information is releasable under FOIA, but requests for such information should be processed in accord with the October 10, 2001 Attorney General's memorandum and should consider use of FOIA exemptions two, three, four, and seven.[291]

On February 17, 2005, USDA promulgated a protection policy for SBU information, which is different from SSI because it "contains information that is not security-related but is still sensitive in terms of its risk of exposure."[292] This information is to be protected and encrypted for transmittal in accord with OMB Circular A-130 and NIST guidance, some of which is specified. All employees and contractors with a "need to know" must sign a nondisclosure agreement and are subject to penalties of noncompliance. Information may be processed for FOIA claims, but it should be considered for protection in light of the Attorney General's memorandum. SBU is defined as in CSA, but without identifying the source as the CSA.[293]

Western Area Power Administration (WAPA). The Western Area Power Administration, (WAPA), an entity of the U.S. Department of Energy,[294] issued guidance for handling sensitive information that it said conforms with Department of Energy policy.[295] "OUO information," it declared, "must ... be unclassified; could be used to damage government, commercial or private interests; [and] be exempt

---

[290] "USDA, "Departmental Regulation Number: 3440-002 Subject: Control and Protection of "Sensitive Security Information," at [http://www.fas.org/sgp/othergov/usda3440-02]. Although risk analysis is required, no reference was made to using NIST-promulgated security standards or methodology to determine risk level and security level.

[291] Regulation 3440-002, op. cit.

[292] "Sensitive But Unclassified (SBU) Information Protection," Chapter 10, Part 2, DM 3550-002, Feb. 17, 2005.

[293] "Conditional Access to USDA Sensitive but Unclassified Information," Nondisclosure Agreement. Attached to DM 3550-002.

[294] According to WAPA, "Western Area Power Administration markets and delivers reliable, cost-based hydroelectric power and related services within a 15-state region of the central and western U.S. We're one of four power marketing administrations within the U.S. Department of Energy whose role is to market and transmit electricity from multi-use water projects. Our transmission system carries electricity from 55 hydropower plants operated by the Bureau of Reclamation, U.S. Army Corps of Engineers and the International Boundary and Water Commission." Available at [http://www.wapa.gov/about/default.htm].

[295] This was identified as "WAPA P 471.1, "Identifying and Protecting Official Use Only Information," that states Western's intent to follow DOE Order 471.3, "Identification and Protection of Official Use Only Information"(Susan DeBelle, " 'Official Use' Info Requires Special Care," *Closed Circuit*, May 28, 2004, vol. 26, no. 11, [http://www.wapa.gov/media/cct/2004/may28/26no114txt.htm]).

from disclosure under the Freedom of Information Act."[296] All such documents must be marked and protected as directed "in the DOE *Manual for Identifying and Protecting Official Use Only Information*."[297] Even information releasable under FOIA should be protected if it is sensitive (such as "total flow on a specified grouping of transmission lines maps and environmental impact statements that were previously posted on the Internet.") Specifically, for such information, it recommends posting " a summary of the information on the Internet; or provid[ing] information that will enable a reader to request a copy of the document. This will give you an opportunity to determine whether or not the requester has a legitimate need for the material."[298] Protections should be applied to information that meets certain criteria, including the technology-related dimensions of whether it contains "details about critical operating facilities, systems or vulnerabilities"; could have questionable impacts if "it inadvertently reached an unintended audience"; could provide"details concerning physical or cyber security measures"; could be "dangerous if it were used in conjunction with other publicly available information"; could be used "to target Western staff, facilities or operations"; or could "increase the attractiveness of a critical infrastructure asset as a target."[299]

Agencies That Use Unique Definitions

Some agencies have developed their own definitions of sensitive information that do not reference either the CSA or NIST-based standards.

Department of Defense. DOD uses the following definition for SBU: For "[a]ccess within the Department of Defense, the criteria for allowing access to SBU information are the same as those used for FOUO information, except that information received from the Department of State marked SBU shall not be provided to any person who is not a U.S. citizen without the approval of the Department of State activity that originated the information."[300] "For official use only" information is for unclassified information and "is applied to information that may be exempt under one or more of the other eight exemptions [to FOIA, the first exception is for classified information]."[301] However, marking it FOUO does not automatically qualify it for an exemption from FOIA. Access is granted to those with

---

[296] DeBelle, op. cit.

[297] The manual expires Apr. 9, 2007, according to [http://ornl.gov/doe/doe_oro_dmg/doectrlfrms.htm]. It is not readily available to permit review if it contains definitions of sensitive.

[298] DeBelle, op.cit.

[299] DeBelle, op. cit.

[300] "Interim Guidance on Safeguarding and Controlled Unclassifed Information," Attached to *Interim Information Security Guidance,"* from Stephen A. Cambone, Undersecretary of Defense, Memo for Secretaries of the Military Departments, et al., Apr. 16, 2004, p. 6.

[301] Attachment to Cambone, op. cit., p. 2.

a need for such access, and such information should be stored in locked files and unauthorized disclosure will be punished by "appropriate disciplinary action."[302]

Department of the Army. The Department of the Army uses the term "Technical controlled unclassified information," pursuant to P.L. 98-94, for data "that disclose critical technology with military or space applications. This includes any blueprint, drawing, plan, instruction, computer software and documentation, or other technical information that can be used or be adapted to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning such equipment."[303]

Department of Energy. The DOE uses the term "official use only" for "sensitive" information that is unclassified. As one of its responses to the recommendations of the Commission on Science and Security in the 21st century, the DOE said it prepared "...a new Official Use Only (OUO) Information Order [completed in June 2002 and current through April 2007], aimed at addressing the issue of 'Sensitive, But Unclassified Information' through the establishment of three information types (classified, unclassified and Official Use Only.)"[304] "To be identified as OUO, information must be unclassified; have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities" and fall under at least one of FOIA exemptions two through nine, Access to documents marked OUO is limited to persons who need it to perform their jobs or other DOE-authorized activities. Documents need to be protected as described in DOE M 471.3-1, and administrative penalties may be imposed on DOE employees for improperly marking or releasing a OUO document. These provisions are applicable to all DOE elements and contractors.[305] An official with DOE's Safeguards and Security Policy staff interpreted DOE's rules with respect to SBU science and technology information, which, he said, encompasses such things as "facilities, personnel, programs, materials, security, safety assessment, vulnerabilities, and the sensitive subjects list."[306] Officials charged with categorizing information are to take the following "considerations" into account when deciding if information is sensitive: "suitability — what does it do for the person, organization, Department; sensitivity — how can it be used by an adversary?; risk —

---

[302] Attachment to Cambone, op. cit., pp. 3-4.

[303] "Controlled Unclassified Information (CUI)" powerpoint slide show, produced by Department of the Army, op. cit.

[304] DOE, "Commission on Science and Security in the 21st Century, DOE accompanied by Recommendations," June 20, 2002. The statement referenced the DOE document *Subject: Identifying and Protecting Official Use Only Information*, DOE Order M 471.3-1, Apr. 9, 2003 (which is current through Apr. 2007).

[305] See also "Subject: Identifying and Protecting Official Use Only Information," DOE Order O 471.3, Apr. 9, 2003. See also "Identifying and Protecting Official Use Only Information," pp. 4, 6 in *DOE Information Classification and Control Policy Communique*, Feb. 2004.

[306] Ray Holmer, "Sensitive Information on the Web, an Information Security Perspective," STIP Meeting May 1, 2003.

what are the chances of an adversary using the information?; consequences — what could happen if an adversary used the information?"[307]

DOE also maintains a Sensitive Subjects List, used largely by affiliated national laboratories, that identifies sensitive information deemed significant to U.S. national security. It is an internal DOE list to be used to identify fields that require a U.S. export license for a foreign national. Topics included relate to nuclear weapons and nuclear fuel cycle, rockets, missiles, and delivery systems; conventional arms and other defense-related technology; chemical and biological weapons; advanced scientific computers and software; and business sensitive (proprietary) information.[308]

Nuclear Regulatory Commission. The Nuclear Regulatory Commission issued rules for "Safeguards Information" (SGI) — that is, unclassified sensitive information deemed too sensitive for public release. The proposed rule, issued in February 2005, said that SGI needs to be protected from unauthorized disclosure under section 147 of the Atomic Energy Act of 1954 as amended. The proposed rule expanded the scope of information included and made more rigorous standards and requirements for background checks and fingerprinting for those who have a "need to know" to see the information.[309] The definition was promulgated in a release issued on May 11, 2005: "While SGI is considered to be sensitive unclassified information, its handling and protection more closely resemble the handling of classified confidential information than other sensitive unclassified information."[310] "Sensitive unclassified information," according to NRC,

> is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.). Information about a licensee's or applicant's physical protection or material control and accounting program for special nuclear material not otherwise designated as Safeguards Information or classified as National Security Information or Restricted Data is required by 10 CFR 2.390 to be protected in the same manner as commercial or financial information, i.e., they are exempt from public disclosure.[311]

Federal Energy Regulatory Commission. The Federal Energy Regulatory Commission (FERC) issued a final rule outlining access procedures to critical energy infrastructure information (CEII), an SBU category it uses. CEII is technical information submitted from companies and utilities during regulatory proceedings. Before September 11, 2001 most of this information was made public.

---

[307] Holmer, op.cit.

[308] DOE Sensitive Subjects List (revised June 2001), available at [http://www.llnl.gov/expcon/SSL.pdf].

[309] Nuclear Regulatory Commission, "Protection of Safeguards Information," Proposed Rule, *Federal Register*, Feb. 11, 1005, pp. 7196-7217, cited in "NRC Proposes New Rule on Unclassified Safeguards Info," *Secrecy News*, Feb. 11, 2005, [http://www.fas.org/sgp/news/2005/02/fr021105.html].

[310] NRC "Information Security," May 11, 2005, available at [http://www.nrc.gov/what-we-do/safeguards/info-security.html#safe].

[311] "Information Security," May 11, 2005.

FERC's position is that CEII includes only information that is exempt from disclosure under FOIA. It also said it developed a process to allow requests to be made for information that is not already publicly available under FOIA, but also will keep sensitive infrastructure information out of the public domain in order to help deter terrorist attacks. The rule noted that the FOIA exemptions most likely to apply to CEII are exemptions two, four, and seven.[312]

Appendix B. Illustrations of Federal Information Systems Created To Transmit Sensitive But Unclassified Information

Federal agencies have started to develop information systems to share SBU information and data among themselves and with state and local first responders. Some of these were mandated by statute. The major legal authorities include the Homeland Security Information Sharing Act, section 892 of P.L. 107-296, which required the development of information sharing procedures for certain types of homeland security information; Homeland Security Presidential Directive (HSPD-7), which required DHS to produce a national infrastructure protection plan summarizing initiatives to share information among public and private sectors; the issuance in August 2004 of executive orders to strengthen terrorism information sharing standards,[313] establishment of a National Counterterrorism Center;[314] as well as passage in December 2004 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, which required the establishment of an information-sharing environment (ISE) and ISE council to exchange terrorism information among pubic and private entities.

Government Accountability Office (GAO) Inventory

The GAO reported to Congress in September 2004[315] that its survey showed that nine federal agencies[316] had developed 34 networks to share information in support of homeland security functions. These include networks such as DHS's Critical Infrastructure Warning Information Network (CWIN). Five agencies, DHS, DOD, DOJ, State, and Treasury managed 18 networks (17 operational and one in development) for SBU information. (SBU "is a generic term used to describe unclassified information that is (1) not required by law to be made available to the public, and (2) sufficiently sensitive to restrict access from public disclosure, but not

---

[312] "Federal Energy Regulatory Commission, Critical Energy Infrastructure Information," Feb. 21, 2003. *Federal Register*, Mar. 3, 2003, vol. 68, no. 41, pp. 9857-9873. For secondary analysis, see [http://www.openthegovernment.org/article/articleview/50/1/16].

[313] E.O. 13356, "Strengthening the Sharing of Terrorism Information to Protect Americans," Aug. 27, 2004.

[314] E.O. 13354, "National Counterterrorism Center," Aug. 27, 2004.

[315] Government Accountability Office, *Information Technology: Major Federal Networks That Support Homeland Security Functions*, Sept. 2004, GAO-04-375.

[316] Departments of Agriculture, Defense, Energy, Health and Human Services, Homeland Security, Justice, State, Treasury, and the Environmental Protection Agency, pp. 50-51.

sensitive enough to warrant a classified designation."[317]) Of these, 11 were networks that shared information internally only within an agency, 2 were networks that shared information only with other federal agencies, and 5 networks shared information with state and local government agencies or the private sector.[318]

Most of the systems permit information dissemination on a "need-to-know" basis. GAO catalogued many of these requirements and responses in its report *High Risk Series: An Update,* released in January 2005.[319] See also the aforementioned CRS Report RL32597.

Other Federal Information Systems

Since the GAO inventory, additional information systems have been identified that exchange SBU information.[320] For instance, DHS is developing a "Homeland Security Information Network" that will utilize the Joint Regional Information Exchange to share SBU and classified information with state and local personnel and the private sector. It was reported in February 2004 that there were about 1,000 users.[321] Other networks over which SBU information exchange occurs include the "Unclassified but Sensitive Internet Protocol Router Network," a government network between DOD users;[322] and the "Terrorist Threat Integration Center (TTIC) TTIC Online system," a DHS information network for disseminating classified domestic and international terrorist information from 14 U.S. government agencies, which is "being updated to support collaboration and information sharing at varying levels, from Top Secret to Sensitive But Unclassified."[323] There is also the "Multi-State Anti-Terrorism Information Exchange" (MATRIX), a regional system covering 13 states, including Alabama, Connecticut, Florida, Georgia, Kentucky, Louisiana, Michigan, New York, Oregon, Pennsylvania, South Carolina, Ohio, and Utah, which exchanges "sensitive terrorism-related information among members of the law enforcement community."[324]

---

[317] *Information Technology: Major Federal Networks*, op, cit., p. 12.

[318] *Information Technology: Major Federal Networks*, op. cit., p. 31.

[319] GAO 05-207, op. cit., pp. 15-20.

[320] For additional details on these types of information sharing systems, see Relyea and Seifert, op. cit.

[321] "Homeland Security Information Network to Expand Collaboration, Connectivity for State and Major Cities," DHS press release, Feb. 24, 2004.

[322] Discussing an Inspector General Report on this topic: [http://www.stormingmedia.us/76/7615/A761583.html].

[323] Statement for the Record of John O. Brennan, Director Terrorist Threat Integration Center on "The Homeland Security Advisory System: Improving Preparedness Through Effective Warning before the House Select Committee on Homeland Security," Feb. 4, 2004.

[324] "State of Georgia Homeland Security Bulletin on MATRIX," Aug. 1, 2003, Georgia's Homeland Security Bulletin No. 20-03.

The Federal Bureau of Investigation in the Justice Department uses a system called "Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive but Unclassified (SBU) level."[325] It also "has secure connectivity to the Regional Information Sharing Systems network (riss.net)." Reportedly, LEO has about 30,000 users, including state and local law enforcement members. "LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence." The system also provides access to "Intelligence Information Reports" at the Law Enforcement Sensitive classification level. "[t]he FBI posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area." Reportedly, "The FBI will use an enhanced LEO as the primary channel for sensitive but unclassified communications with other federal, state and local agencies. LEO and the DHS Joint Regional Information Exchange System (JRIES) will also be interoperable."

DHS also launched a system in April 2004 for "state and local emergency officials across the country ... [to] ... trade preparedness tips, training ideas and best practices right from their desks on the Lessons Learned Information Sharing system, LLIS...."[326] Reportedly, emergency officials will have to complete an online authorization process to view the site, whose content "must meet DHS standards for 'sensitive, but unclassified information....'"

FEDTeDS

In addition to these networks, the federal government created FEDTeDS, the Federal Technical Data Solution. It is a way to transmit and disseminate security-sensitive or sensitive but unclassified acquisition material related to solicitations found in *FedBizOpps.gov* [http://www.fedbizopps.gov].[327] It is a collaborative effort among agencies, led by DOD, the Coast Guard, and the Integrated Acquisition Environment (IAE) eGovernment initiative under the President's Management Agenda. Vendors are to use this system to prepare sensitive information in bids or proposals. Such information can include specifications, drawing and plans for federal installations, schedules, procedures, and so forth. More than 90 federal agencies are reported to disseminate SBU acquisitions-related materials during the

---

[325] Statement of Maureen A. Baginski, Executive Assistant Director, Intelligence, Federal Bureau of Investigation, before the House of Representatives Select Committee on Homeland Security, Aug. 17, 2004.

[326] Caitlin Harrington, "DHS Launching Web Page for Emergency Officials to Trade Tips," *Congressional Quarterly Homeland Security*, May 15, 2004.

[327] According to Federal Technical Data Solution (FEDTeDS), sensitive data with respect to the solicitation phase of procurement via the Internet includes "information related to operations, weapons systems and plans, transit authority, structures, individuals and services essential to the security and management of a facility, including telecommunications, electrical power, building facility structure layout, Gas and oil storage/transportation, water supply, emergency services, and the continuity of operations" ("Federal Technical Data Solution (FedTeDS) Providing Federal Agencies a System to Safeguard 'Sensitive But Unclassified' Acquisition Information," *IAE Bulletin*, No. 4, July 17, 2003).

solicitation phase of procurement via the Internet; this system serves approved users. It became operational on February 19, 2003.[328]

Section 1016 (b) of P.L. 108-458, the National Intelligence Reform Act (S. 2845, H.Rept 108-796), the intelligence overhaul bill responsive to the 9/11 commission report, called for development of an "information sharing environment" that would link information systems and allow users to share information between agencies, between levels of government, and with the private sector. It also mandated a principal officer and executive committee to create rules and regulations to implement the information sharing environment. Reportedly, DHS's Homeland Security Advisory Council plans on releasing a report that calls for more information exchanges from federal to state, local, and private sectors, and vice versa.[329]

The aforementioned GAO High Risk Series Report concluded that despite these kinds of efforts, "a great deal of work remains ... to improve homeland security information sharing, including establishing clear goals, objectives, and expectations for the many participants in information-sharing efforts; and consolidated, standardizing, and enhancing federal structures, policies, and capabilities for the analysis and dissemination of information."[330]

---

[328] Lisa Cliff, "E-Gov Corner: FedTeDS (Federal Technical Data Solutions)," *Federal Acquisition,* July 2003, and "Federal Technical Data Solution (FedTeDS) Providing Federal Agencies a System to Safeguard 'Sensitive But Unclassifed' Acquisition Information," IAE Bulletin No. 4, July 17, 2003. See also "Business Opportunities," *Homeland Security IntelWatch,* Mar. 11, 2004, p. 1.

[329] Joe Fiorill, "U.S. Panel Seeks Broad Information-Sharing Changes to Improve Antiterrorism Efforts," *NTI, Global Security Newswire,* Dec. 13, 2004.

[330] GAO 05-207, op. cit., p. 20.