Testimony of
Harry Hammitt
Editor/Publisher, Access Reports
House Subcommittee on National Security, Emerging Threats and International Relations
March 2, 2005

My name is Harry Hammitt. I am the editor/publisher of *Access Reports*, a biweekly newsletter on the Freedom of Information Act, open government issues, and informational privacy issues. I have attached a copy of the newsletter relevant to the topic of this hearing. I have been editing *Access Reports* for almost 20 years. During that time I have become the expert's expert on the Freedom of Information Act. I am the primary editor of *Litigation Under the Federal Open Government Laws*, considered the best source on the subject for requesters and plaintiffs. I have been a contributing editor to *Government Technology*. I am a former president of the American Society of Access Professionals, a Washington-based professional association of people who work with FOIA and privacy issues, and a current board member of the organization. I have taught FOIA training sessions for ASAP and various other public interest organizations and have spoken on these issues in various forums in the U.S. and internationally. Before becoming editor of the newsletter, I worked at the Consumer Product Safety Commission processing FOIA requests, and at FOI Services, a company that makes requests on behalf of business clients. I have both a master's degree in journalism from the University of Missouri-Columbia, and a law degree from George Washington University Law School. I think the combination has served me well in understanding and writing about information access issues.

I want to thank the subcommittee for inviting me to testify on this important and timely information issue. I hope to provide an overview of some of the programs that have developed, indicate where they came from and how and why they developed, and then close with my assessment of how these programs impact information policy.

In my judgment, these programs cause more harm than good. They are:

- too ill-defined and broad, and, as a result, are subject to abuse and substantial over-use;

- a solution to a problem that may not exist and based on the dubious proposition that secrecy will make us more safe rather than less safe and that agencies and companies will not use secrecy to hide their own mistakes and avoid public scrutiny;

Historical Perspective

The existence of such undefined categories of restricted information has accelerated during the Bush administration. But all these categories did not somehow appear fully formed after September 11, 2001. Several have existed for years. The term "sensitive, but unclassified" goes back at least to the Reagan administration, and has a statutory basis in the Computer Security Act of 1987. The concept of critical infrastructure information appeared during the Clinton administration and its protection today is modeled on legislation concerning the Y2K problem that Congress passed in 2000. Such terms as "sensitive security information," "sensitive homeland security information," and "critical energy infrastructure information" are more recent additions to the information lexicon. What all these categories have in common is their ill-defined nature.

The Card Memo

In March 2002, White House Chief of Staff Andrew Card sent a memo[1] to all agencies concerning the need to safeguard sensitive but unclassified information pertaining to homeland security. Because such undefined information did not qualify for classification on national security grounds, Card attached two short memos from Laura Kimberly, Acting Director of the Information Security Oversight Office,[2] and Richard Huff and Daniel Metcalfe, Co-Directors of the Justice Department's Office of Information and Privacy,[3] explaining possible FOIA exemptions that could be used to

[1] Andrew H. Card, Jr., Assistant to the President and Chief of Staff, Memorandum for the Heads of Executive Departments and Agencies; Subject: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002).
[2] Laura S. Kimberly, Acting Director of the Information Security Oversight Office, Memorandum for Departments and Agencies (Mar. 19, 2002).
[3] Richard Huff and Daniel Metcalfe, Co-Directors, Office of Information and Privacy, Department of Justice, Memorandum for Departments and Agencies (Mar. 19, 2002)

withhold such information. Primary among them was Exemption 2,[4] which allows an agency to withhold records "related solely to the internal personnel rules and practices of an agency." Over the years, courts have stretched these words so they now allow an agency to withhold records where disclosure could lead to circumvention of a law or regulation. The Justice Department memo reminded agencies to consider using Exemption 2 for such sensitive but unclassified information on the untried theory that disclosure would allow a requester to circumvent a law or regulation. Although it said little about the scope of the problem, the Card memo was the first White House policy directive concerning the need to protect sensitive unclassified information and was certainly a primary factor in moving the development of such policies forward.

Sensitive Security Information

Sensitive security information is one of the few such categories with a statutory basis. In November 2001, Congress passed the Aviation and Transportation Security Act, creating the Transportation Security Administration. That statute defines sensitive security information as information describing air carrier screening procedures, airport or air carrier security programs, maritime transportation security procedures, or other related transportation security matters. It prohibits the disclosure of such information if the TSA Administrator determines disclosure would "be detrimental to the safety of passengers in transportation."[5] The Homeland Security Act of 2002 expanded this to cover information that "would be detrimental to the security of transportation." A May 2004 *Federal Register* notice set out 16 categories of information from traditional security plans to security directives and included "other information" that TSA at its discretion determined should be withheld. This statutory authority is structured so that it qualifies as an Exemption 3[6] statute under FOIA. Exemption 3 is a catch-all provision in FOIA that allows agencies to withhold records whose disclosure is prohibited or restricted by a provision in another statute as long as that statute either provides no discretion on the part of the agency or identifies specific categories of information to be withheld.

[4] 5 U.S.C. 552(b)(2).
[5] 49 U.S.C. 114(s)(1) and 49 U.S.C. 40119(b)(1).
[6] 5 U.S.C. 552(b)(3).

communities, but are not available to a wider audience and are not available at all in electronic form.

The worst-case scenarios controversy dovetailed with a related concern then being brought up in Congress – the possibility that computers would fail to properly recognize the date change when the calendar moved from 1999 to 2000, potentially causing massive equipment failures. An important part of assessing the potential for such trouble was to encourage the private sector to share its concerns about vulnerabilities with the government. To encourage such information-sharing, Congress passed Y2K legislation that prohibited disclosure of any such voluntarily-submitted information under FOIA and also excused the private sector from any potential liability if their products did fail as a result of the date change.

The issue of protecting critical infrastructure information more generally was still being discussed when the Bush administration took office and some form of legislation might well have been passed in the next year or two. But the attacks of September 11, 2001 tied the issue more closely to terrorism. Instead of being an issue about protecting confidential business information, it was now rolled into the push to protect the nation from future terrorist attacks. As part of the Homeland Security Act of 2002, the House of Representatives passed a provision allowing the Department of Homeland Security to protect voluntarily-submitted critical infrastructure information. In the Senate, public interest groups helped craft a provision that, while allowing such voluntary submissions, would allow outside challenges, based on the D.C. Circuit's decision in *Critical Mass v. NRC*,[8] as to whether or not specific submissions did indeed qualify as critical infrastructure information. The amendment, offered by Sen. Robert Bennett (R-UT) and Sen. Patrick Leahy (D-VT), was adopted by the Senate but was dropped in conference, leaving the House provision as the final version.

The Department of Homeland Security issued proposed regulations concerning the voluntary submission of critical infrastructure information in 2004, although the regulations are not yet final. At least one controversial suggestion in the regulations was that critical infrastructure information could be submitted to other agencies and could then be passed along to Homeland Security. The statutory language appears to

[8] *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992).

contemplate that such submissions can only be made to the Department of Homeland Security and public interest groups were concerned that allowing other agencies to collect the submissions expanded the provision's reach.

A recent article in *SecurityFocus*[9] looks at how the submission process has worked so far and notes that at least the information technology industry is still wary of the program and has yet to submit any information. Although the information is protected from public disclosure, industries are more concerned about its potential wide dissemination within government. Sean Moulton, a policy analyst at the public interest group OMB Watch, explained to *SecurityFocus* the concerns of the public interest community. He indicated that industry had been given more protection than public interest groups thought was warranted, yet industry was still uncomfortable submitting such information. He pointed out that "I really find it troubling that it's industry driving the process and not the government driving the process, when it's the public who has a stake in this. It's the public who will be harmed if these infrastructures are attacked."[10]

Critical Energy Infrastructure Information

The Federal Energy Regulatory Commission has created its own category of sensitive information, known as critical energy infrastructure information, and has faced its own specific problems which it has had to finesse. The Commission oversees the energy industry and holds a number of administrative proceedings involving companies and utilities in that area. As a part of these hearings, the Commission requires submission of technical information, including infrastructure information. Generally, most of this information would be public when used in a proceeding. However, after September 11, 2001, FERC moved more aggressively than virtually any other agency to remove critical energy infrastructure information from the public domain. The agency's regulations define CEII as information that is exempt from FOIA and submitted to the agency by private parties about proposed or existing critical infrastructure that relates to

[9] Poulsen, Kevin. "U.S. Info-Sharing Initiative Called a Flop, *SecurityFocus*, Feb. 11, 2005.
[10] Ibid.

the production, generation, transportation, transmission or distribution of energy and which "could be useful to a person planning an attack on critical infrastructure."[11]

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 suggested potpourri of possible exemptions. These include Exemption 2, which protects information the disclosure of which could allow someone to circumvent a law or regulation, Exemption 7(E), which allows a law enforcement agency to withhold information that would reveal investigative methods and techniques, and Exemption 7(F), which allows a law enforcement agency to withhold information the disclosure of which could endanger the physical safety of an individual. The agency also suggested that the information could be withheld under Exemption 4, which protects confidential business information, because a terrorist attack would clearly cause a company economic harm. The other problem is that FERC wanted to continue 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 non-disclosure agreement. It is difficult to see how information that was previously public could become non-public based solely on agency regulations.

The Impact on Disclosure of Such Categories of Information

These 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 a solution to a problem that may not even exist and are based on what I consider to be an antithetical proposition in our democracy – that, when in doubt, always favor secrecy over openness. That is not to say that some government information should not remain secret; we can all agree that some information, such as troop movements in time of war, for instance, should be kept secret. But when our government fosters the attitude that there are vast undefined categories of information that must be, at a minimum, safeguarded by agencies, it does a grave disservice to the

[11] 18 C.F.R. § 388.113(c) (68 Fed. Reg. 9857, 9870 (March 3, 2003)).

ideal of an open democratic society. It is paternalistic for government to assume that people cannot handle the availability of such information.

Government officials say these designations, like "sensitive but unclassified," or "for your eyes only," have no legal status and cannot be used to deny access under FOIA. While this is true on a technical level, it is hard to believe that when agency personnel are faced with a document with such a designation they are not going to think twice before agreeing to disclose such a document. In other words, such a designation sets off red flags that suggest the record merits withholding. The problem with the Justice Department's memo attached to the Card memo is that it outlines a strategy for withholding information that perhaps should have been released. When a record says "sensitive, but unclassified," the first step for agency personnel is likely to try to figure out which FOIA exemption can be applied.

For years, most outside observers have complained that too much information is classified. The annual reports of the Information Security Oversight Office consistently show that the number of classification determinations, whether at the original or derivative level, continue to go up every year. But the national security classification scheme provides several potential remedies for forcing the disclosure of classified information. These include a mandatory declassification review, most often in conjunction with an FOIA request, or a review by the Interagency Security Classification Appeals Panel (ISCAP). Review by ISCAP, created by Executive Order 12958 issued by President Clinton, has resulted in further disclosure of previously classified information in a significant majority of cases. However, the number of cases heard by the panel is relatively small and resort to it is not a practical option for many requesters.

When it comes to the undefined categories of information that are the subject of today's hearing there are no remedies short of litigation, probably under FOIA. While the government's collection of recommended exemptions has not been thoroughly tested, at least two U.S. district court judges have accepted some combination of these claims.[12] Further, the expanded deference shown by the D.C. Circuit in litigation[13] over disclosure of the identities of individuals who were detained in the immediate aftermath of

[12] See *Living Rivers, Inc. v. Bureau of Reclamation*, No. 2:02-CV-644TC (D. Utah, Mar. 25, 2003) and *Coastal Delivery Corp. v. Customs Service*, No. 02-3838 WMB (C.D. Cal., Mar. 14, 2003).
[13] *Center for National Security Studies v. DOJ*, 331 F.3d 918 (D.C. Cir. 2003).

September 11, 2001, suggests that courts would likely be sympathetic to the government's arguments when it came to withholding information based on concerns about possible terrorist use. There is no administrative appeal aside from that available under FOIA. This means, realistically, that there are fewer checks against the improper denial of such undefined categories of information than exist for classified national security information.

When such real or imagined restrictions are placed on information, there are consequences for internal dissemination as well, a problem that particularly concerned the 9/11 Commission. The national security classification system has designations for "Top Secret," "Secret," and "Confidential" information. Not only must such designations be made only by individuals who have the delegated authority to do so, once classified that information may only circulate with specific limitations. To see a record classified as "Top Secret," an individual must have a top secret classification clearance. Those whose clearances are no higher than "Secret" or "Confidential" are not supposed to use information classified at a "Top Secret" level. And individuals who have no security clearance aren't supposed to have access to any classified information.

The same kinds of restrictions likely exist in practice for records labeled "sensitive, but unclassified" or "sensitive security information" or any of the other undefined categories under discussion here. Once these kinds of restrictions are put into place, they impose severe limitations on dissemination which may rob them of much of their value in the first place. While such limitations within the federal government can be disruptive enough, further dissemination to state and local officials, who in most instances are likely to have no clearance at all, may be that much more restricted. If information is to be useful, it must be available.

The wisdom of these programs is suspect at best, but once in place it is difficult to completely do away with them. There are, however, several options that might at least make them more tolerable. Using the national security classification system as a model, the definition of what constitutes sensitive information could be spelled out much more specifically and dissemination could be based on categories, with dissemination of the most sensitive information being more restricted than for information of a less sensitive nature. A standard definition of sensitive information could be crafted and its use could

be limited so that only agencies that would legitimately be expected to have such information would be able to categorize records as sensitive. Some degree of flexibility in defining subcategories, such as critical energy infrastructure information, could be given to those agencies whose information fits into that specific category. Regardless, any restrictions on such subcategories could be no broader than allowed under the overall definition of what constitutes sensitive information. Agencies using any of these categories should be required to implement standards designed to maximize public access to such information to ensure that the concept of sensitive information is not used as a broad brush to withhold or restrict information more generally.

Further, 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. 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 obsession with protecting such information because under some scenario it might be of use to a terrorist, fails to consider the value of the information itself. Vulnerabilities in our infrastructure should not be broadcast to potential enemies, but should not be hidden under a basket either. A good analogy for fostering greater public disclosure is how open source software code works in the computer world. When such code is openly available, individuals tinker with it in an effort to improve it or to expand its utility. When such programs are closed, they stagnate rather than expand. Bridges or roads or manufacturing facilities that are vulnerable will not be fixed because their vulnerabilities are hidden. They are much more likely to be fixed, and thus become less useful as an end goal for terrorists, because individuals and groups put pressure on government or business to fix them. We need to be less fixated on the potential harmful use of information and more cognizant of the way in which we can use that information to achieve a result that makes us both safer from potential attack and safer because vulnerabilities have been addressed. As a nation we cannot very well address vulnerabilities when we do not know they exist.

These undefined categories of information stifle the availability and use of information. They expand the universe of information agencies are likely to withhold from the public solely because of their designation. They also restrict the availability of information within government and particularly between levels of government. One of the lessons of the 9/11 Commission's report is that information is most useful when it is available. Various bureaucratic gate-keeping regimes that slow or halt the flow of information, or worse still, hide its existence, are detrimental to our available knowledge base and, ultimately, do us more harm than good.

Thank you for allowing me the opportunity to share my view with the subcommittee. If I can answer any questions or provide more information, I will be glad to do so.