Statement by **Thomas S. Blanton**, National Security Archive, George Washington University
March 2, 2005

Hearing on "Emerging Threats: Overclassification and Pseudo-classification"

2154 Rayburn House Office Building
Subcommittee on National Security, Emerging Threats, and International Relations
Committee on Government Reform
U.S. House of Representatives

Mr. Chairman, and members of the Committee, thank you for this opportunity to speak with you about the growing problem of **government secrecy and the danger it poses to our security**. This Subcommittee has become a model for the Congress as a whole in its diligent oversight of a difficult problem, and I applaud your commitment to air diverse views and to question conventional thinking.

I have reviewed in detail the record of your hearing on August 24, 2004, to which my own organization, the National Security Archive, contributed a reader of declassified documents entitled "Dubious Secrets," featuring General Pinochet's drink preferences (scotch and pisco sours) and a joke terrorist attack on Santa Claus (the secret was that the CIA occasionally has a sense of humor). Mr. Chairman, you asked the question whether overclassification was a 10% problem or a 90% problem, and your witnesses provided some remarkable yardsticks. The deputy undersecretary of defense for counterintelligence and security confessed that **50% of the Pentagon's information was overclassified.** The head of the Information Security Oversight Office said it was even worse, "even beyond 50%." The former official who participated in the Markle Foundation study cited by the 9/11 Commission on information sharing stated that 80-90% (at least in the area of intelligence and technology) was appropriately classified at first, but over time that dwindled down to the 10-20% range.

My own experience is in the realm of declassified national security information. The National Security Archive ranks as probably the most active and successful non-profit user of the Freedom of Information Act: We have filed more than **30,000 Freedom of Information and declassification requests** in our nearly 20 years of operations, resulting in more than six million pages of released documents that might otherwise be secret today (some of them have in fact been reclassified, but the government won't tell us which ones). We have published more than half a million pages on the Web and other formats, along with more than 40 books by our staff and fellows, including the Pulitzer Prize winner in 1996 on Eastern Europe after Communism. We won the George Polk Award in April 2000 for "piercing self-serving veils of government secrecy." We have partners in 35 countries around the world doing the same kind of work today, opening the files of secret police, Politburos, military dictatorships, and the Warsaw Pact, and leveraging openness in both directions.

My own estimate of overclassification in the United States today tends towards the high end of your 90% range, Mr. Chairman. Let me put on the record here several expert assessments to support this view. For example, the distinguished former Solicitor General of the United States who prosecuted the Pentagon Papers case, Dean Erwin Griswold, wrote in the *Washington Post* (15 February 1989) that: *"It quickly becomes apparent to any person who has considerable experience with classified material that there is **massive overclassification** and that the principal concern of the classifiers is not with national security, but with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past."*

Senator Daniel P. Moynihan's commission on reducing and protecting government secrecy quoted Rodney B. McDaniel, a career Navy officer and executive secretary of President Reagan's National Security Council, who estimated in 1991 that **only 10% of classification was for *"legitimate protection of secrets*."** The Moynihan report contrasted this view with that of the then-head of the Information Security Oversight Office, Steven Garfinkel, who stated that overclassification was only a 10% problem. (1997 Report, p. 36) As this Subcommittee heard in August, Mr. Garfinkel's successor has now moved the official estimate above 50%.

A Cox News Service report last summer (21 July 2004) headlined "Lawmakers Frustrated By Delays In Declassifying Documents," quoted the Republican former governor of New Jersey and then-chair of the 9/11 Commission, Thomas H. Kean, as saying, ***"Three-quarters of what I read that was classified shouldn't have been"*** – a 75% judgment. The material Mr. Kean was reviewing included the most recent and sensitive terrorism-related intelligence and counterterrorism information. The same Cox article quoted Senator Trent Lott (R-Miss.) on his frustration with the Senate Intelligence Committee report on Iraq, as reviewed by the CIA: *"The initial thing that came back was absolutely an insult and would be **laughable if it wasn't so insulting**, because they redacted half of what we had. A lot of it was to redact a word that revealed nothing."*

I agree with Senator Lott and Governor Kean: national security secrecy is skyrocketing, but like the ballistic missile defense system, it cannot tell the real threat from the decoys. Let's start with the core statistics, or least the most recent ones available, provided by the Information Security Oversight Office in last year's report to the President. New classification decisions are up from 9 million in 2001, to 11 million in 2002, to 14 million in 2003. If you look at that ISOO data all the way back to the first year in which it was collected – 1980 – you will discover that **the number of new secrecy decisions in 2003 is the highest ever recorded, higher even than the peak years of the Cold War in the mid-1980s**.

Tracking the same ISOO data since 1980, we can also see **the rise and fall of declassification in the 1990s**. The ISOO reports show many years of low levels (around 20 million pages per year) until the numbers leap in 1995, stay at the 200 million page level for three years, and then plummet down under 50 million pages a year now. I think it's fair to say that President Clinton's executive order on secrecy produced the declassification of more historic national security secrets than all previous presidents put together. But now, the system is almost completely out of whack – a point that ISOO's director made at your August hearing.

At least the national security classification system has **formal checks and balances**. By all the evidence of overclassification, these checks do not work very well, but they do exist. They **desperately need strengthening**. I'm thinking not only of ISOO, that lean machine of a small, well-trained professional staff providing audits and oversight, within its limited means, of a vast and sprawling system. There is also the Interagency Security Classification Appeals Panel (ISCAP), which has ruled for openness in some 60% of its cases (there's another marker on the overclassification gauge), although the total number of cases is quite small and involves mostly historical rather than current information. There is also the Office of Management and Budget requirement, first included in appropriations bills in the 1990s, that agencies add up and report their classification costs (the CIA's are still classified, of course) – thus giving us a benchmark number and some sense of comparative expense to the taxpayer. These numbers, over $6.5 billion in fiscal 2003, remind us that every secrecy decision generates a stream of direct costs to the taxpayer, in addition to the indirect costs of inefficiency and information asymmetries.

Likewise, the executive orders governing classification have been around long enough that a cottage industry of insiders and outsiders have developed expertise on how the system works or ought to work. And at least since the 1974 amendments to the Freedom of Information Act, the courts have provided some guidance on classification. In general, the courts defer to the executive (to a fault, I would argue), but along the way, the extra levels of review during litigation almost always force out information that the agencies originally withheld. In other words, **we lose the final decision, but we get documents**.

What's most alarming is that the new forms of secrecy, the "pseudoclassifications" like Sensitive But Unclassified (SBU) or Sensitive Security Information (SSI) or Sensitive Homeland Security Information (SHSI), have **no such checks and balances**. Where is the **audit agency**, tracking the basic data on the number and extent of new restrictions? Where is the **appeals panel**, overriding the reflexive instincts of agencies? Where is the **cost reporting**, or do the agencies lack any clue as to how much the secrecy costs them? Where is the **cost-benefit analysis** inside agencies, or do they not see the double-edged sword inherent in secrecy? Where are the **bureaucratic centers of countervailing power**, pressing for declassification? Where are the court cases, or will judges continue blind deference to executive judgments? Where is the Congress, when the President's lawyers assert unilateral authority over secrecy, detentions, interrogations, and energy policy, among many other topics?

The National Security Archive's experience with pseudoclassification is not encouraging. Among our many projects, we are pursuing the public release of the actual primary sources cited and quoted by the 9/11 Commission, and we have been on the receiving end of an object lesson in reflexive pseudosecrecy at the Transportation Security

Administration. For example, last year we asked for the five Federal Aviation Administration warnings to airlines on terrorism in the months just prior to 9/11 – warnings that were quoted in the 9/11 Commission report and discussed at length in public testimony by high government officials. The TSA responded by denying the entire substance of the documents under five separate exemptions to the Freedom of Information Act, and even withheld the unclassified document titles and Information Circular numbers as "Sensitive Security Information." When we pointed out that the **titles, dates, and numbers were listed in the footnotes to the number one best-selling book in the United States**, the 9/11 Commission report, the TSA painstakingly restored those precise digits and letters in its second response to us, but kept the blackout over everything else.

We have heard from officials at the Department of Justice that these new pseudoclassifications 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.

As William Leonard of ISOO pointed out at the GovSec Expo (July 29, 2004), SBU protection regimes still exist that date back to the Cold War, and none have been officially discarded. The government, instead, is adding regimes year after year, Mr. Leonard remarked, *"without any regard to what's been done before to a point where I'm concerned today that if you wanted to identify the person in the government or outside the government who understands all the various protection regimes, understands what all the requirements are, understands what all the standards are – that person doesn't exist."*

This dynamic is fundamentally what's wrong with the Markle Foundation recommendations for the SHARE network that were embraced by the 9/11 Commission and about which you heard from Mr. Bill Crowell at your August 2004 hearing. I read his testimony and the two editions of the Markle report with great interest, because the group seems to have begun with the assumption that you share, Mr. Chairman, that the "need to know" secrecy culture is working against our security. But **the group's recommendations do not actually challenge the "need to know" culture. Instead, they embrace the SBU attitude,** the official-use-only elitism. The language in Mr. Crowell's testimony and in the underlying reports gives a remarkable amount of attention to the ways that the SHARE system would help agencies control and track and audit employees, preventing leaks and authenticating information, keeping the data in the hands of only the relevant players.

That's the key phrase. Mr. Crowell's direct quote before this Subcommittee was: *"While certain information, particularly about sources and methods, must be protected against unauthorized disclosure, the general mindset should be one that strives for broad sharing of information with all of* ***the relevant players*** *in the network."* Who exactly decides who are the relevant players? Where do we draw the line? Are firefighters included in but not health inspectors? Epidemiologists but not general practitioners? Power plant managers but not the plant's workers? First responders but not neighbors? **Aren't we right back where we started at the need to know?** What will stop the SHARE system from turning into the mother of all pseudoclassifications? The strength of our open society is the free flow of information but the SHARE concept looks more like the Soviet GOSPLAN.

We could spend billions of dollars implementing the computer networks necessary for SHARE, or we could invest a few million in real openness and government accountability. President Bush nominated members for the Public Interest Declassification Board but did not include the Board's $600,000 allowance in his budget. We could establish **an independent review board with a small staff like ISOO at every major federal agency for a million dollars each per year**, less than the cost of our excellent military marching bands.

The number one lesson of 9/11 is that the "relevant players" include the public, front and center. As the staff director of the Congressional Joint Inquiry on 9/11 found, *"The record suggests that, prior to September 11th, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort:* ***an alert and informed American public.*** *One need look no further for proof of the latter point than the heroics of the passengers on Flight 93 or the quick action of the flight attendant who identified shoe bomber Richard Reid."* After all, the only part of our national security apparatus that actually prevented casualties on 9/11 was the citizenry – those brave passengers on Flight 93 who figured out what was going on before the Pentagon or the CIA did, and brought their plane down before it could take out the White House or the Capitol.

Look at the case of the Unabomber, the Harvard-educated terrorist who blew up random scientists with letter bombs. Years of secret investigation turned up nothing but rambling screeds against modernity and the machine, and only after the madman threatened more violence unless his words were published, did the FBI relent and give the **crank letter file to the newspapers**. The *Washington Post* and the *New York Times* went in together on a special section to carry the 35,000 words in 1995, but the key paper was the *Chicago Tribune*, read at the breakfast table in a Chicago suburb by the bomber's brother, who said, sounds like crazy Ted, guess I'd better call the cops.

How did we catch the Washington sniper? The police had been chasing a white van for weeks with no luck, and finally changed the description to a blue sedan based on an eyewitness report. They refused to give out the license plate number (because the sniper would then change the plates, of course); but finally an unnamed police official took it upon herself to leak the license number at midnight, local radio and TV picked it up, and a trucker was listening who saw a blue sedan in a rest area in western Maryland. He checked the plate number, and bingo, **within three hours of the leak they arrested the sniper**. Openness empowers citizens.

The entire 9/11 Commission report includes only one finding that the attacks might have been prevented. This occurs on page 247 and is repeated on page 276 with the footnote on page 541, quoting the interrogation of the hijackers' paymaster, Ramzi Binalshibh. Binalshibh commented that if the organizers, particularly Khalid Sheikh Mohammed, had known that the so-called 20th hijacker, Zacarias Moussaoui, had been arrested at his Minnesota flight school (he only wanted to fly, not to take off or land) on immigration charges, then Bin Ladin and KSM would have called off the 9/11 attacks. And wisely so, because news of that arrest would have alerted the FBI agent in Phoenix who warned of Islamic militants in flight schools in a July 2001 memo that vanished into the FBI's vaults in Washington. The Commission's wording is important here: **only "publicity" could have derailed the attacks.**

This is why Ms. Carol Haave, the deputy undersecretary of defense, framed the problem wrongly at your August 24 hearing. She testified, *"In the end, this is a discussion about risk. How much risk is the nation willing to endure in the quest to* ***balance protection against the public's desire to know?*** *It's a complex question that requires thought and ultimately action."* She and the Pentagon have missed the point. We are not balancing protection against the public's desire to know. The tension is actually between bureaucratic imperatives of information control versus empowering the public and thus making us more safe. Yes, there are real secrets that must be protected, but the lesson of 9/11 is that we are losing protection by too much secrecy. The risk is that by keeping information secret, we make ourselves vulnerable. The risk is that when we keep our vulnerabilities secret, we avoid fixing them. In an open society, it is only by exposure that problems get fixed. In a distributed information networked world, secrecy creates risk – risk of inefficiency, ignorance, inaction, as in 9/11. As the saying goes in the computer security world, **when the bug is secret, then only the vendor and the hacker know – and the larger community can neither protect itself nor offer fixes**. Publicity is not a SHARE network limited to relevant players. Publicity is TV, the newspapers, the Internet, and the highly efficient information distribution system that is our open society. That is our strength, not our weakness.

So how do we put countervailing pressure on the secrecy system, and on the new SBU systems, to force publicity, to empower the public? We can start the way the framers did, with checks and balances. **If you create a power center for creating and holding secrets, like the new intelligence czar, then you need a counter center for declassifying secrets**. The Moynihan commission, for example, recommended setting up a formal Declassification Center based at the National Archives and staffed by an interagency group with delegated powers from their agencies. Their performance would be measured by their openness. Just such a group served the Congress well during the

Iran-contra investigations by reviewing and declassifying more than 30 thick volumes of testimony and documents in record time, with enormous benefits for government accountability and without damage to national security.

Another model is the Public Interest Declassification Board authorized in the intelligence reform bill last year. Not all the members have yet been named, so the jury is still out on whether this Board will meet the expectations of Senators Lott and Wyden, for example. But **every previous experience with a statutory independent review board has been a major success**, pushing out of the system the secrets that do not need keeping. These include the Assassination Records Review Board, the State Department's historical advisory committee, and the Interagency Working Group on Nazi and Japanese War Crimes. Every agency needs a review board like these, with authority in statute, with scholars and former officials doing the oversight, with regular reporting requirements and open meetings. The model we should not follow is that of the CIA, where the advisory committee has no statute behind it and, by allowing its recommendations to remain confidential, has voluntarily given up what little leverage it might have had.

One of William Leonard's recommendations is that the new secrecy systems have to be coordinated with the old ones. He makes the valid point that it would be a major reform and **potential restraint to have a common set of standards** across all agencies in place of the differentiated, culture-driven, idiosyncratic standards that have arisen in the multiple secrecy regimes. Such differences create huge uncertainties among officials about what behavior is expected and how much information to share.

Even part of the CIA agrees with this critique. For example, a 1977 study by the CIA of its own codeword compartments (declassified in 2002) found that the proliferation of compartments had deleterious psychological effects that "seem to diminish rather than enhance security," and recommended that the DCI abolish all existing compartments and replace them with one uniform Sources-and-Methods compartment. The intelligence community is moving in this direction (witness the 1999 abolition of the COMINT codewords UMBRA, SPOKE, MORAY and the TALENT-KEYHOLE codeword ZARF); but bureaucratic inertia and turf-consciousness pose major obstacles to the rational consolidation of SBU and secrecy rules today. Yet, the secrecy skeptic in me thinks that perhaps **centralization is not the cure-all**, that perhaps the diversity of our bureaucracy is actually a protection for dissenting views, for multiple perspectives, and for alternative policy options.

More important than centralization, **we must build into all of our secrecy systems multiple provisions for cost-benefit analysis, audits, oversight offices, cost accounting, and independent reviews**. We must limit the number of officials who have the power to wield the secret or SBU stamp. We must increase the number of officials whose jobs and careers depend on opening information. We must **change the internal bureaucratic incentives**, by tying promotions and raises to declassification and information sharing, while providing real penalties for knee-jerk secrecy and information hoarding.

There are interesting examples of carrot-and-stick provisions on government openness both abroad and at home. We could look to Sweden, for example, where the bishop of Stockholm, a public official, had to pay a fine (nearly $2,000) last year for violating the open records law, by withholding letters from priests in the state-supported church about their problems and challenges. Or we could look to Florida, where an Escambia County school board member went to jail for a week in 2003 for refusing to provide a public record to a Pensacola mother. The name of that school board member is now a household word among officials in Florida, deterring bad behavior. It's a more difficult question, but one we must address, about how to deter absurd classification decisions like the CIA's claim (now upheld by a federal court) that it can declassify the 1997 intelligence budget figure with no damage to national security, but the 1947 number still must be secret (Steven Aftergood testified in detail about this case at the August 24, 2004 hearing). Secrecy decisions like this one actually undermine the credibility of the entire information security system and make our real secrets less safe.

In the final analysis, of course, it is openness that empowers our citizens, weeds out the worst policy proposals, ensures the most efficient flow of information to all levels of law enforcement, makes a little more honest the despots who are our temporary allies against terrorism, and keeps our means more consistent with our ends.

Thank you, Mr. Chairman, and I look forward to any questions you may have.