

Joseph Masco  
 Department of Anthropology  
 The University of Chicago

*Ethnografeast III: Ethnography and the Public Sphere*  
 Lisbon, Portugal June 20-23, 2007

### **The Nuclear Public Sphere**

The power of the secret in contemporary American society is difficult to overestimate. Currently, the logics and policy goals of the national security state – including the evidence for war, the terms of extraordinary rendition and the “detainee,” as well as the surveillance of U.S. citizens -- have all been formally designated as “secrets” under a discourse of imminent threat. The “newness” of the “war on terror,” however, masks the deep structure of this logic and the profound mutation in the nature of the state produced by the advent of the atomic bomb and the accompanying expansion of state secrecy devoted to protecting it. Indeed, the invention of the national security state after World War II transformed America into a new kind of secret society, one in which state power rests to an unprecedented degree precisely on the ability of officials to manage the public/secret divide through the mobilization of threat. This “secrecy/threat matrix” marks all state secrets as the equivalent of the atomic secret, making revelation not just a matter of politics but of the life or death of the nation-state. The Cold War arms race – founded on the minute-to-minute possibility for nuclear war – installed the secrecy/threat matrix as the grounds for a new species of politics in the United States. I argue that the transformation of the United States from a counter-communist to a counter-terrorist state formation has reconstituted and amplified this secrecy/threat matrix, revealing aspects of its essential form in a highly distorted public sphere.

Consider, for example, a recent exchange I had with the U.S. Department of Energy (DOE) over reproduction access to an image from the U.S. nuclear program archives. I was looking for a version of a photograph illustrating the casing and non-nuclear parts of a modern thermonuclear weapon. Several versions of the image I had in mind were used in public hearings I attended in the 1990s to illustrate the challenges of the Science Based Stockpile Stewardship (SBSS) program within the DOE – a more than \$70 billion effort to maintain the Cold War nuclear arsenal without underground nuclear testing. Thus, through the 1990s, and even as the U.S. waged pre-emptive

war to eliminate the threat of weapons of mass destruction in Iraq in 2003, it was committed to building a state-of-the-art nuclear arsenal via SBSS.<sup>1</sup> The photograph of a dismantled nuclear device, known as the B61, was used by Los Alamos weapons scientists and DOE officials in the early and mid-1990s to document the difficulty of dealing with aging weapons parts (Masco 2004). Under the SBSS program, each of the 6000-7000 components in a nuclear weapon has a specific surveillance program devoted to it, and the photographic illustration of those parts was a central means of articulating the difficulty of surveillance and engineering the bomb without underground testing. This specific image was therefore a key part of the campaign to justify the expense of SBSS in the post-Cold War period. As a scholar with a book then in production that dealt, in part, with the evolution of the stockpile stewardship program at Los Alamos, and the evolving logics of U.S. national security programs after the Cold War, I had hoped to find a copy of this image to reproduce in my book (see Masco 2006). My intent was to use the photograph as an illustration of the SBSS program, as well as the public discussions that accompanied it in the post-Cold War nuclear policy debates around Los Alamos National Laboratory.

Along these lines, I asked a variety of agencies within the federal government for a copy of the image, forwarding a low-resolution copy that I had scanned from SBSS publicity materials. Usually quite helpful and forthcoming with media requests, their reactions were at times both curious and funny: A Los Alamos representative said, that while the laboratory designed the nuclear device known as the B61, the image could not be found within their media archives. He speculated first that perhaps it was an Air Force image, and then suggested that the photograph would be more likely the purview of Sandia National Laboratory, which is involved in engineering the casing and non-nuclear components for U.S. nuclear weapons. Sandia, however, did not respond to any of my media requests. Pantex, which is charged with dismantling U.S. nuclear devices, also could not locate the image and referred me to Lawrence Livermore National Laboratory, which produced a similar image of a Livermore designed nuclear device, known as the B83. Lawrence Livermore National Laboratory referred me to the DOE in Washington, where my request for the image was gently but promptly refused. Pushing a bit further, I inquired about why the image, or one like it, was not available to a scholarly project and received the following email:

In regards to the B-61 picture, after September 11, 2001, a review was conducted of our visuals library. As a result some images are not being released due to security concerns.

For many readers, this undoubtedly seems to be a logical outcome. After all, images of nuclear weapons are historically the quintessential “state secret” – the very reason for having an elaborate system of classification and information control in the United States. But what is the actual status of this photograph?

Here, we might consult one of the most widely distributed Department of Energy publications of the post-Cold War period – *Closing the Circle on the Splitting of the Atom* (DOE 1994). On page 20 one will find the image in question (see Figure 1):

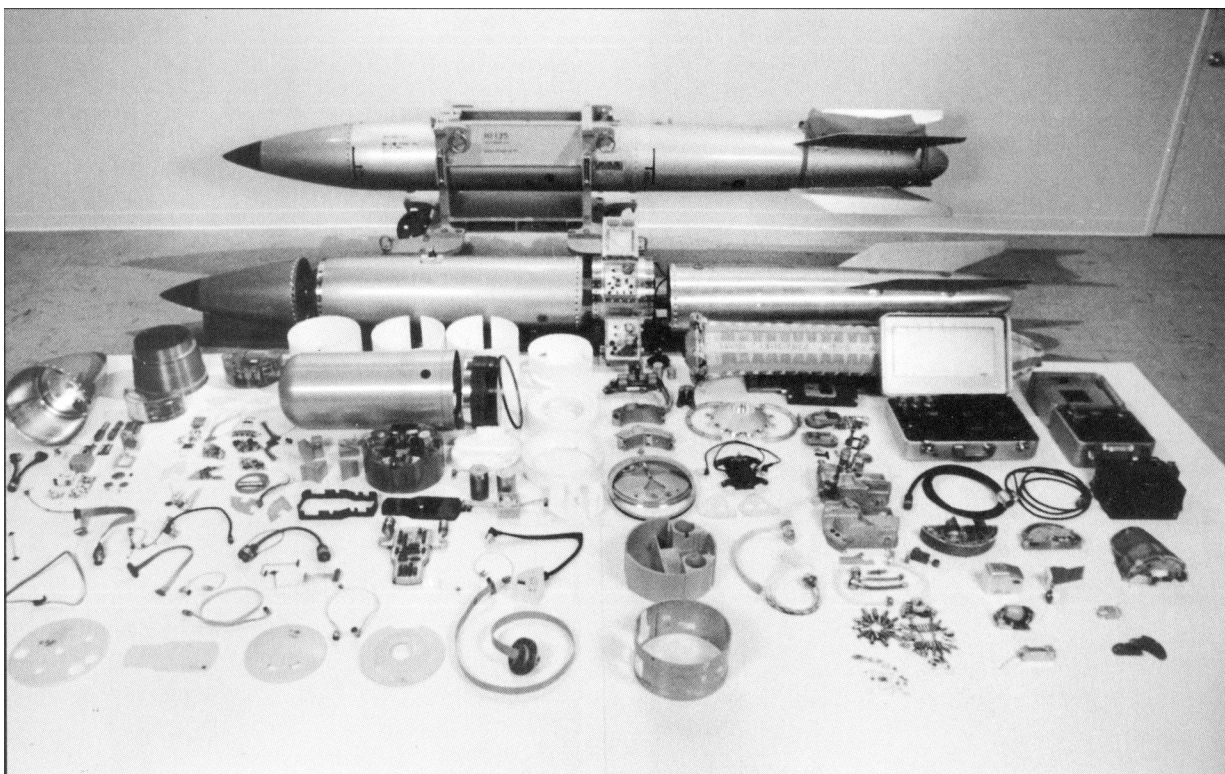


Figure 1: Dismantled B-61 nuclear weapon from *Closing the Circle* (DOE 1994).

The caption for this image reads (DOE 1994: 20):

An example of a completed nuclear weapon and its component parts. At top, an intact B-61 nuclear bomb. At bottom, the assemblies and subassemblies that comprise this weapon. Dozens of facilities across the country engage in different processes and contribute specific parts to the production of nuclear weapons.

Thus, as of 1994, this image was in the public domain (and reproduced in a second edition from 1996). You might then conclude that it is the September 11<sup>th</sup> attacks and the declaration of a “war on terror” that has provoked the transformation of this image from a public to a nonpublic state. After all, the “war on terror” was founded in fear of the “wmd” and the need to prevent the flow of information that might help terrorists or President Bush’s “axis of evil” -- Iraq, Iran, or North Korea – in their nuclear ambitions. However, the *Closing the Circle* document remains available today for public download from the DOE at:

<http://legacystory.apps.em.doe.gov/pdfpic.asp?doc=close>.

You might think this is simply an oversight, a bureaucratic failure to pull an old document from a government website after the post-9/11 reconstitution of the national security state as a counter-terrorist formation. But consider the following photographs (Figures 2 and 3) from the Los Alamos National Laboratory’s Bradbury Science Museum, which I took in 2005 (Please note the inset photographs in each figures).

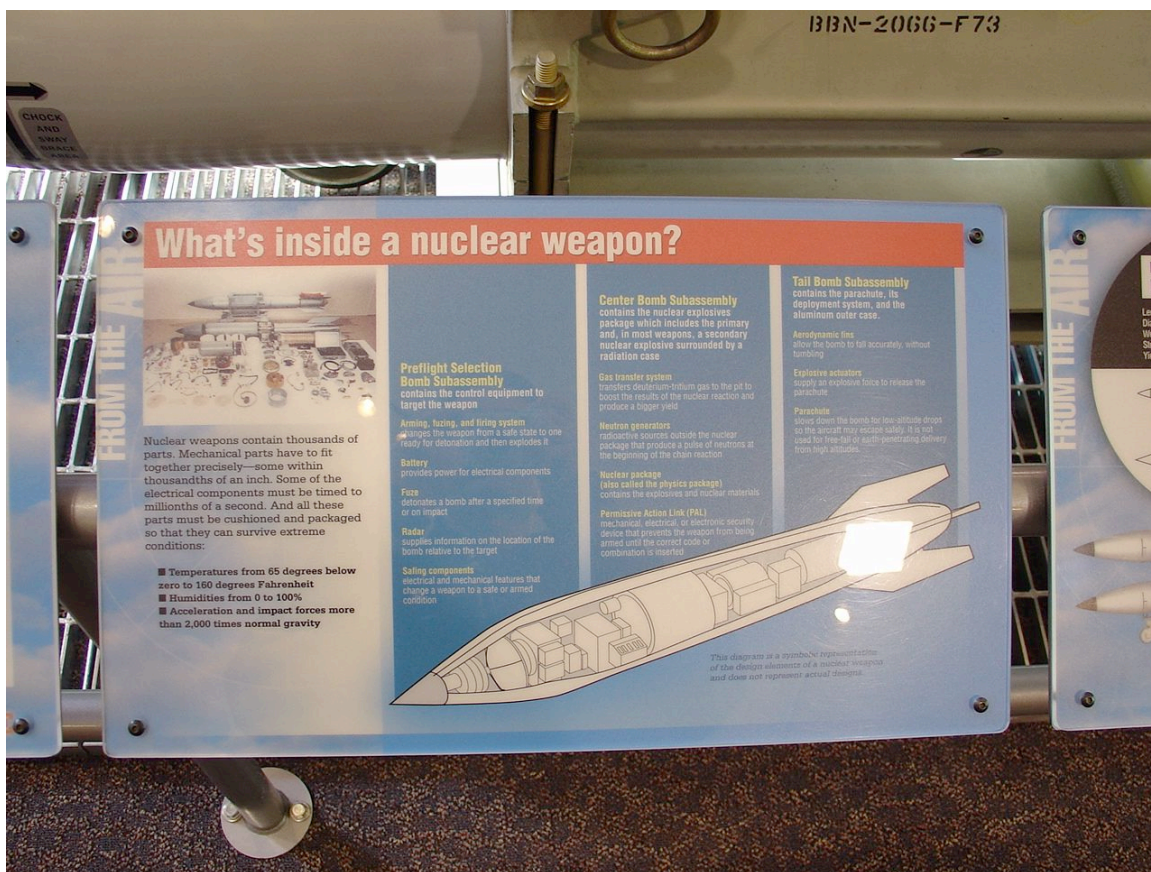


Figure 2: Nuclear Weapons Exhibit at the Bradbury Science Museum (Photograph by Joseph Masco)

Figure 2 documents the same B-61 image as presented in the *Closing the Circle* publication, but also adds a great deal of detail, contextualizing the photograph within the larger design complexity of a nuclear device. The exhibit describes the basic components of a modern thermonuclear bomb, emphasizing the complexity of the bomb as machine: thousands of parts need to be matched together “within thousandths of an inch” and timed to operate within “millionths of a second” while experiencing extremes in temperature, humidity, and acceleration.



Figure 3: B83 Exhibit at the Bradbury Science Museum  
(Photograph by Joseph Masco)

Figure 3 presents another dismantled weapon, the B-83, as well as pictures of its delivery method, parachute, and airdrop. The text also offers a statistical portrait of the bomb, marking the length, weight, age, and explosive power – in the “megaton range” – of the B83 as “the most powerful weapon in the U.S. arsenal.”

Thus, it is not the image itself or a detailed description of the bomb that is a subject of official concern, which would explain why the DOE would not allow it to be reproduced in my book. Presented at the Los Alamos National Laboratory Museum, one might then think that it is an issue of proximity, of being at the center of U.S. nuclear science where information can be controlled via the surveillance of the security system itself. However, one can find another version of the B-83 photograph (see Figure 4) currently on display at the National Atomic Museum in Albuquerque, an institution devoted to telling the story of U.S. nuclear energy programs as well as the bomb. The National Atomic Museum is affiliated with the Smithsonian and is currently located in the museum district of Albuquerque – adjacent to the natural history and fine arts museums, a prime tourist destination. In addition to images of the dismantled weapon and diagrams of its operation, the casing of an actual B-83 bomb is on display, as well as a pictorial exhibit of how it would be delivered via Air Force jets. Thus, a proximity to nuclear expertise and the mechanisms of security within a national laboratory are not a necessary criteria for the presentation of detailed nuclear weapons information, as The National Atomic Museum is staffed by volunteers and is not monitored by the security teams of a national weapons laboratory.



Figure 4. B-83 nuclear weapon exhibit at the National Atomic Museum.  
(Photograph by Joseph Masco)

Thus, we seem to be at a logical quandary – the images of dismantled B61 and B83 bombs are simultaneously marked as security risks and widely distributed. The bomb seems to be both core object of the security state – with the official desire to protect the nuclear secret energizing the entire system of military-industrial compartmentalized knowledge – and the bomb is subject to its own forms of publicity. Indeed, consider this final image (see Figure 5) from the Bradbury Science Museum, which asks not what is inside an atomic bomb but “what’s in the U.S. nuclear Stockpile?”

# What's in the U.S. Nuclear Stockpile?

The stockpile, also called the nuclear arsenal, is one part of the U.S. defense strategy. The term nuclear weapons refers to the explosive warheads and the bombs and missiles that can deliver them to enemy targets.

U.S. nuclear strategy relies on a combination of aircraft-delivered bombs (identified with the prefix B) and cruise missiles, intercontinental ballistic missiles, and submarine-launched missiles (whose warheads are identified with a W). This combination remains the strongest, most flexible, and most survivable form of deterrence. Each type of warhead is designed to meet a variety of military requirements, the constraints of the delivery vehicle, and the conditions the weapons might experience—called the stockpile to target sequence.

The distinction between strategic (long-range, more powerful) weapons and tactical (short-range, less powerful) ones is important to military strategists and to arms control negotiators. Tactical weapons deployed near a country's borders are considered a greater threat because of the shorter time available for the country to respond to an attack.

All the weapons in the enduring, active U.S. stockpile are listed below, and some of them are displayed inside this railing. Those not displayed are either too large or their size or shape is classified. Information about the nuclear warheads, their delivery vehicles, and carriers is provided along the railing.



## AIR

Designation	Description	Delivery Vehicle	Design Laboratory
B61	Tactical and strategic bombs	F-15, F-16, B-52, B-2	Los Alamos and Sandia
B83	Strategic bombs	B-52, B-2	Livermore and Sandia
W80-1	Tactical cruise missile	B-52	Los Alamos and Sandia

## LAND

Designation	Description	Delivery Vehicle	Design Laboratory
W78	Strategic warhead	Minuteman III	Los Alamos and Sandia
W87	Strategic warhead	Peacekeeper	Livermore and Sandia
W62	Strategic warhead	Minuteman III	Livermore and Sandia

## SEA

Designation	Description	Delivery Vehicle	Design Laboratory
W76	Strategic warhead	SS missile on Trident submarine	Los Alamos and Sandia
W88	Strategic warhead	SS missile on Trident submarine	Los Alamos and Sandia
W80-0	Tactical warhead	Cruise missile on Tomahawk submarine	Los Alamos and Sandia

### How Do Nuclear Weapons Fit into the U.S. Defense Strategy?

During the Cold War, the U.S. maintained a triad of air-, land-, and sea-based strategic nuclear forces, described above, primarily as a deterrent to the Soviet Union. The U.S. and our allies now face many potential threats from terrorists and nation states developing weapons of mass destruction and ballistic missiles.

As a result, the U.S. is moving toward a new triad:

- OFFENSE**—nuclear and nonnuclear air, land, and sea strike capabilities.
- DEFENSE**—protection against missile and aircraft attacks through interception, concealment, warning, redundancy, mobility, hardening, and other measures.
- INFRASTRUCTURE**—a responsive system of laboratories and plants that design, develop, and produce the materials needed for offensive strikes and defensive protection.

This strategy is to assure our allies of our security commitments and dissuade others from threatening us.



Figure 5: Nuclear Stockpile Exhibit at the Bradbury Science Museum  
(Photograph by Joseph Masco)

The exhibit presents the designations of the bombs (capital B) and warheads (capital W) in the U.S. arsenal (B61, B83, W80-1, W78, W87, W62, W78, W88, W80-0), the delivery methods (aircraft, cruise missiles, intercontinental ballistic missiles, submarine launched missiles), the design laboratories of each weapon (Los Alamos, Livermore, Sandia), as well as the strategic and

tactical deployments on air, land, and sea that make up the nuclear triad (of bombers, missiles, submarines). Thus, the make and model, as well as delivery method and conceptual placement of each device within the U.S. nuclear arsenal are presented here as public knowledge – which again raises the question: what kind of information does the disassembled B-61 bomb photograph constitute?

The B-61 photograph is both widely circulated – available to anybody interested enough in nuclear weapons policy and science to download a file from the DOE website, or willing to visit either of the two major museums devoted to the U.S. nuclear program – and yet, also restricted “due to security concerns.” If it were a “classified” image, then the directors of the two museums could today be charged with espionage, as could the head of the DOE for posting materials to the web. And tourists, with snapshots, such as the ones I took in 2005, from either of the museum displays would be in immediate violation of federal law and subject to arrest. And you as the dear reader of this text would also be in possession of a nuclear secret, holding in your hands an object of potential espionage subject to military action. But since the museum and Internet materials have not been pulled from circulation, my exchange with the DOE begs the question: how can information be simultaneously in the “public domain” and a “state secret”?

The B-61 photograph is now an example of an expanding category of government information known as “sensitive but unclassified.” Within this designation, information is not officially classified as a state secret, and thus subject to all the laws about handing such information; it is simply withheld from public circulation. I want to argue that the evolving use of the SBU designation reveals an important aspect of the transformation of U.S. national security culture from a counter-communist to a counter-terrorist state formation. It also marks a significant evolution in the power of the bomb -- not as a military tool but as a cultural-political form -- to define contemporary domestic politics, illustrating a profound expansion of the national security state after the post-Cold War period (1991-2001). A new concept of official secrecy was established in the immediate aftermath of World War II that increasingly positioned citizens as a threat to state security, and separated huge parts of government from either public scrutiny or citizen participation. Indeed, the atomic bomb was mobilized in this moment to create a new kind of security state, one linking the official declaration of imminent threat to an

expansive project of compartmentalized secrecy. The Bush Administration's "war on terror" has sought to revitalize and extend this project, mobilizing the "wmd" and expansive secrecy to enable new agendas, both foreign and domestic. Before interrogating the logics of "sensitive but unclassified" knowledge, however, I want to explore how this "secrecy / threat matrix" has transformed the nature of the secret (and in so doing, the relationship between citizens and the state).

With the 1946 Atomic Energy Act and the 1947 National Security Act, the United States effectively removed huge areas of governmental affairs from citizens' purview. These acts formally installed a new security state within the United States, constituting a rather fundamental change in the nature of American democracy. The Atomic Energy Act created the first kind of information – nuclear weapons data -- that did not need to be formally classified: it was "born" that way, while the National Security Act created whole new governmental institutions (the Central Intelligence Agency as well as the National Security Agency – the first of what would become 16 intelligence agencies in the U.S.) which by charter would not be publicly accountable to citizens. Created in peacetime, the new agencies and logics marked the establishment of a permanent war economy as well as a fundamental commitment to state secrecy in the United States. Rationalized as an effort to protect military secrets about the atomic bomb in an uncertain world, these acts inaugurated a split between national security and state security in the U.S., with citizens implicitly recognized as a potential barrier to state security policies. The evolving U.S. security state increasingly used nuclear fear after 1945 as a means of reconstituting the line between domestic and international politics to mobilize citizens as Cold Warriors.

While the concept of a "state secret" was not invented during the Manhattan Project, the state structures that were established to build the bomb have subsequently evolved into a unprecedentedly massive infrastructure in the U.S. – so massive in fact, that its sheer scale is difficult to access. Today there is certainly more knowledge that is classified than is not, more knowledge that is produced and locked up in the military industrial state than is offered by all nonmilitary academic literatures. Peter Galison has recently tried to calculate the scale of secret versus public knowledge in the United States, using the Library of Congress as a metric. He offers this perspective (2004:231):

There are 500,000 college professors in the United States – including both two- and four-year institutions. Of course there are others – inventors, industrial scientists, computer programmers – responsible for generating and conveying knowledge, especially technical knowledge. But to fix ideas, four million people hold [security] clearances in the United States, plus some vast reservoir who did in the past but no longer do. Bottom line? Whether one figures by acquisition rate, by holding size, or by contributors, the classified universes is, as best I can estimate, on the order of five to ten times larger than the open literature that finds its way in our libraries.

*The classified universe is five to ten times larger than the open literature.* Produced in the name of citizens who have no access to this knowledge except as employees of the security state, the classified universe is not simply a means of protecting the nation-state from the spread of dangerous military information; official secrecy is a social technology, a means of internally regulating American society. The organizing principle for this system of secrecy is the atomic bomb, which is positioned within the universe of classification as the ideal type of state secret. Indeed, the system of secrecy that developed after World War II was premised on the idea that every thing marked as “classified” had the potential to produce catastrophic results if made public. An important part of the cultural work accomplished by the state’s recitation of nuclear threat in the first decades of the Cold War was to establish this linkage between the “classified” and the “apocalyptic” – merging a bureaucratic system for managing the military industrial economy with images of imminent destruction for the slightest slippage or revelation. By discursively positioning every classified file as potentially an “atomic secret” the state transformed a vast system of secrecy into a fully nationalized system of perception management in the form of the secrecy / threat matrix.

Since 2001, secrecy has been a core tool in transforming the U.S. from a counter-communist to a counter-terrorist state, and is an ever-expanding practice.<sup>2</sup> In a variety of Executive Orders and formal directives, the Bush Administration has required each agency of government to increase its control of information.<sup>3</sup> According to government audits, there were nine million formal classification decisions in 2001 but over 16 million in 2004, an increase of 75%. Moreover, the rate at which records that are over 25 years old are declassified has fallen by over 75% in the same period. Thus, the past as well as the present is slipping back behind the curtain.<sup>4</sup> The current cost of simply managing secret information in the U.S. is estimated to be over \$7.2 billion a year, involving in one year alone 4007 classification authorities and over 351,150 brand

new classifications decisions (ISOO 2004a and 2004b). Put differently, for every dollar spent on declassification in 2004, \$148 dollars were spent creating new secrets (OpenTheGovernment.Org 2005a). However, these figures only deal with explicit decisions to classify or declassify information, which is a formal regulatory process. “Sensitive but Unclassified” (SBU) information is a potentially larger and more influential category of knowledge. SBU information is not officially classified; as I noted earlier, it is information simply removed from public circulation as if it were.

Officially aimed at protecting information about “critical infrastructure” following the terrorist attacks in 2001, the expanding use of this provision has radically changed the way information is handled within federal agencies. The 2002 Homeland Security Act charged federal employees to “identify and safeguard homeland security information that is sensitive but unclassified” – although the act defined none of its terms, leaving it up to each agency to draw the lines between public access and critical infrastructure. Concurrently, the Department of Justice advised all government agencies to limit the scope of Freedom of Information Acts requests wherever possible – forcing litigation and thus rewriting the intent of the FOIA law. To these ends, the Bush Administration has advocated a “mosaic” theory of information threat to support an expanded use of the SBU category and to fight Freedom of Information Act requests. The mosaic theory assumes that disparate items of information (particularly the innocuous and of no obvious utility to an adversary) can nonetheless be assembled to create a whole that is more powerful than the sum of its parts. Under this theory, any piece of information is potentially a national security threat, as it is the creative linkage across bits of knowledge that is imagined to be dangerous. David Pozen (2005:679) has consequently argued that an aggressive use of the mosaic theory of information synergy produces claims that are “unfalsifiable,” leading inevitably to over-classification. The result of these new laws, practices, and interpretive strategies is obvious: information that flowed relatively freely a few years ago – Environmental Impact Statements of government projects, for example – now fall into this SBU category and are often not available to citizens. The overall strategy of the counter-terrorist state has thus been to replace a presumption of transparency in non-military matters with a more restrictive posture, one that emphasizes non-circulation rather than, or in addition to, formal classification (See

Robert 2006:36-41). It is via the SBU category that much of American society is being implicitly militarized – as keeping basic governmental information from citizens is increasingly normalized, and equated with anti-terrorism.

The most important aspect of the SBU category of information is that it has never been defined by federal law, it is a strategically vague concept that is used differently by each federal agency. A recent study by the Government Accounting Office (2006) found 56 different definitions of SBU currently used within the Federal government, as well as few provisions to identify which (and how many) officials within an agency can designate information as SBU. The SBU designation is today a largely unregulated category within the Federal government. The first SBU concept, which is still used today by the Department of Energy, was written two decades ago by John Poindexter (who was the head of DARPA until the proposed “total information awareness” data mining project forced him to step down in 2002; prior to that, he gained notoriety for his role in the Iran-Contra scandal of the 1980s). In 1986, as President Reagan’s National Security Advisor, Poindexter defined SBU information this way (quoted in Knezo 2003:20):

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

The “related but not limited to” concept here expands the SBU category to include most of governmental work. Recent surveys of the SBU category have suggested that as much as 75% of non-classified government produced information could be designated as Sensitive but Unclassified. From the perspective of the security state, the value of SBU as a category is not only its ambiguity – as literally anything in government can now be separated from the public sphere – it is that there is no formal review process required to designate information as SBU. There is no agency in government charged with regulating SBU information or hearing appeals. It is therefore up to each branch and agency within the federal government to decide how to

draw the line between public accountability and security, allowing near infinite flexibility in standards and logics.

The SBU category effectively expands national security to include any kind of information that might be inconvenient to the execution of state policy. Articulated as an anti-terrorism provision – it was sold to protect “critical infrastructure from terrorist attack” -- the new SBU practices, as well as the laws, regulations, and federal guidance on information management, now position all citizens as potential terrorists. For if having basic information about governmental practices can be constituted as a “threat”, then SBU functions to blur the distinction between the citizen and the enemy. It makes any kind of federal information subject to noncirculation, creating an expansive category between the explicitly classified and the public. Following the declassification campaigns of the immediate post-Cold War Period, and the enormous democratization of information access enabled by the Internet in the last decade, the 21<sup>st</sup> century has thus witnessed a fundamental shift in the idea and mechanisms of openness and transparency in the United States. Consequently, a central part of the conversion of the U.S. to a counter-terrorist state has been an information strategy of non-circulation but also of censoring the existing public record. The National Archives have become an explicit front in the counter-terrorism project, as historical records relating to Presidential Authority, war-authorizations, intelligence on weapons of mass destruction issues, and other military matters going back to the start of the Cold War have been removed, and designated as either SBU or re-classified (ISOO 2006).<sup>5</sup> At least one million pages of previously declassified materials have been pulled from the National Archives.<sup>6</sup> Thus, the past history of the security state as well as its current projects are being subject to new forms of secrecy, which attempt not only to protect ongoing activities but to purge past mistakes and debates from the public record. From the perspective of the counter-terrorist security state, the value of SBU as a category is not only its ambiguity – as literally anything in government can now be separated from the public sphere – it is that there is no formal review process that citizens can take to release information designated SBU. There is no agency in government charged with regulating the use of SBU or hearing appeals. But while an informed citizenry is the first victim of the elaborate secrecy system in the United States, policymakers also suffer.

There is a remarkable moment in Daniel Ellsberg's autobiography (2002: 237-8), in which he describes a conversation with Henry Kissinger, who was on the verge of becoming the Secretary of State in 1969. Ellsberg, the Rand analyst who will eventually leak the top secret U.S. history of the Vietnam War known as the Pentagon Papers to *The New York Times* and *The Washington Post* (see Prados and Porter 2004), is trying to prepare Kissinger for the psychological effects of having access to above top-secret information. He tells Kissinger that, over the coming years, he will feel in order: exhilarated (at the access), then foolish (for what he once thought he knew), then contempt for those who do not have access, then increasing skepticism about the quality of classified information. In the end, he tells Kissinger (Ellsberg 2003: 237-8):

It will become hard for you to learn from anybody who doesn't have these clearances. Because you'll be thinking as you listen to them "What would this man be telling me if he knew what I know? Would he be giving me the same advice, or would it totally change his predictions and recommendations?" And that mental exercise is so torturous that after a while you give it up and just stop listening. I've seen this with my superiors, my colleagues...and with myself...You will deal with a person who doesn't have those clearances only from the point of view of what you want him to believe and what impression you want him to go away with, since you'll have to lie carefully to him about what you know. In effect, you will have to manipulate him. You'll give up trying to assess what he has to say. The danger is, you'll become something like a moron. You'll become incapable of learning from most people in the world, no matter how much experience they may have in their particular areas that may be much greater than yours.

*You'll become something like a moron.* Ellsberg reveals here a rarely commented on aspect of compartmentalized secrecy in the U.S.: that it relies not only on withholding information but also on lying. Individuals must lie in order to protect their own classification level in everyday interactions throughout the system, and thus, distort their social relations to protect the system of secrecy. Knowledge itself thus becomes doubly corrupted: first, because of the effect of compartmentalization on perceptions of expert knowledge as described by Ellsberg, and second, because perception control becomes as important as information management. Deception via classification becomes the internal structure of the security state, which over time works not to underscore the value of information, the assumed effect of a system of compartmentalized classification, but rather to corrode the terms of knowledge and expertise, making individual motivations also suspect.

The modern state form while promoting the idea of a public sphere is, in many respects, founded on the assumption of secrecy. Foucault (1995, 2003) demonstrates that the modern state not only maintains the right to keep secrets but also to subject its citizens to increasingly minute

forms of surveillance. The logic of the panopticon – as a new icon of state power in the 19<sup>th</sup> Century – is of a sovereign that sees without being seen, while the project of population management requires a fine mesh of institutions devoted to measuring individuals and creating statistical portraits of citizens across a wide range of subjects from health, to education, to economy. Thus, Foucault is able to chart a steady progression in the forms of knowledge and intimacy of these state projects from the overthrow of monarchical authority to the early 20<sup>th</sup> century nation-state as the tools of surveillance and technologies of population management increase. Thus, there has always been a profound separation between citizens and the state, and the practice of democracy politics has always been a highly mediated one. Yet, the kind of state produced in the aftermath of World War II – a nuclear armed, global superpower – expands a core principle of the nation-state form – the use of secrecy in the name of collective security – and expands it into a totalizing structure, one that links all aspects of the state in a global counter-formation. The act of secrecy becomes in this post-World War II system not just a technology of state power, a means of orchestrating policy and protecting state interests through withholding information, but rather the basis for a new kind of power. The idea of the “secret” in the Cold War state becomes deployable in and of itself; evoking secret knowledge becomes a means of suggesting greater knowledge, expertise, and understanding than is, in fact, possible. The secrecy / threat matrix is ultimately a perception management project, one that functions to create, protect, and project the idea of a “super-powered state.” In this regard, it is the atomic bomb that inaugurates a new kind of social contract in the United States, one that separates national security as a public discourse from state security as an institutional practice, and that ultimately grounds the power of the state in the ability to destroy or be destroyed.

The “WMD” as a technological form has always promised apocalyptic consequences for the release of technical information. By mobilizing all state secrets as the equivalent of the “atomic secret,” the security state has increasingly consolidated and limited its power to the realm of threat and threat management. The need to add new categories and practices of secrecy after 9/11 to a state that already produces many times over the amount of classified as opposed to open knowledge reveals one long-term effect of the Cold War secret / threat matrix. Official secrecy can now effectively restrict even the most banal forms of government information under

the Sensitive but Unclassified concept. The SBU category overturns the market logics of the “information age” in which information made free was seen as a social good.<sup>7</sup> SBU effectively removes the rest of non-military government from the public sphere, potentially forcing all requests for information to be via the Freedom of Information Act and litigation. The effects of this are widespread not only for systems of accountability in the U.S. but especially for the sciences in which self-censorship is increasingly sought for those working in fields of study that might have infrastructural or military or patent applications. Thus, the broader effect of these policies is to define the public sphere not as an inherent aspect of democratic order but as a fundamental risk to that very order, one that citizens should willingly surrender for their personal safety. For what does it mean when the free flow of information is the exception rather than a rule in a global superpower that is also a self-identified democracy?

Finally, the secret society that is the state is ultimately headless, an effect of both the systematic distortion in the believability of knowledge as it moves up a compartmentalized infrastructure and the demands on individuals to protect perceptions of their position through systematic lying. But there is an even more powerful aspect of state secrecy when taken to the level of the current nuclear state: the “idea” of secret knowledge itself becomes deployable, corrupting public understandings of what is possible and what is not but also giving the executive authority the ability to seem more knowing than they actually are. In the lead up to the invasion of Iraq in 2003, the Bush Administration systematically deployed *the idea* that there were weapons of mass destruction as well as an imminent threat to the U.S.—to enable war. Vice President Cheney, for example, stated in a speech to the Veterans of Foreign War National Convention on August 26, 2002 that there was absolute certainty about the Iraqi threat:

Simply stated, there is no doubt that Saddam Hussein now has weapons of mass destruction. There is no doubt he is amassing them to use against our friends, against our allies, and against us. And there is no doubt that his aggressive regional ambitions will lead him into future confrontations with his neighbors -- confrontations that will involve both the weapons he has today, and the ones he will continue to develop with his oil wealth.<sup>8</sup>

*There is no doubt.* Here is the secrecy/threat matrix in action, for Cheney implies that the intelligence community has documented with perfect clarity not only the technical terms of the Iraqi biological, chemical, and nuclear programs but also the intent of the regime to use them “against our friends, against our allies and against us.” This is not a deployment of actual

knowledge, as the lack of any evidence of weapons in Iraq after the invasion demonstrates, but it is a deployment of the idea of secret knowledge (knowledge that can only be revealed in its conclusions not its substance).

In his presentation to the United Nations in September 2002, Secretary of State Colin Powell was more exacting in his deployment of the secret/ threat matrix.<sup>9</sup> He portrayed an Iraqi biological weapons program that was so advanced it was already capable of threatening the United States. Claiming sources within the Iraqi government, he presented cartoon diagrams of mobile weapons labs (See Figure 6) and satellite imagery of WMD production facilities (See Figure 7). Powell states conclusively:

We know that Iraq has at least seven of these mobile, biological agent factories. The truck-mounted ones have at least two or three trucks each. That means that the mobile production facilities are very few -- perhaps 18 trucks that we know of. There may be more. But perhaps 18 that we know of. Just imagine trying to find 18 trucks among the thousands and thousands of trucks that travel the roads of Iraq every single day....

*We know.* This depiction of mobile “biological agent factories” effectively transforms every truck in Iraq into a potential Weapon of Mass Destruction laboratory.

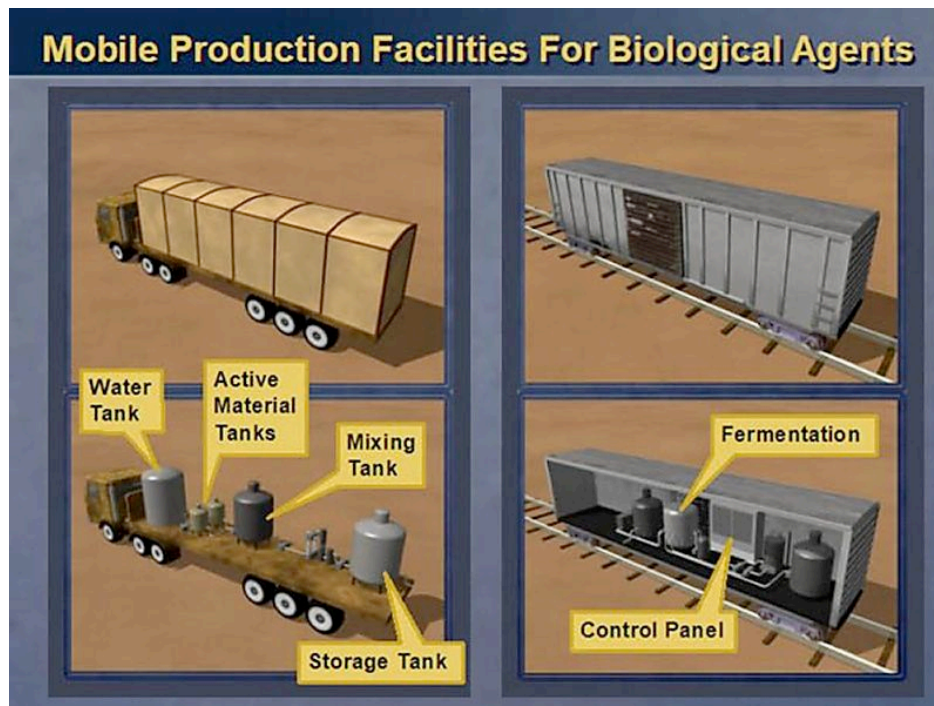


Figure 6: Iraqi Mobile Labs

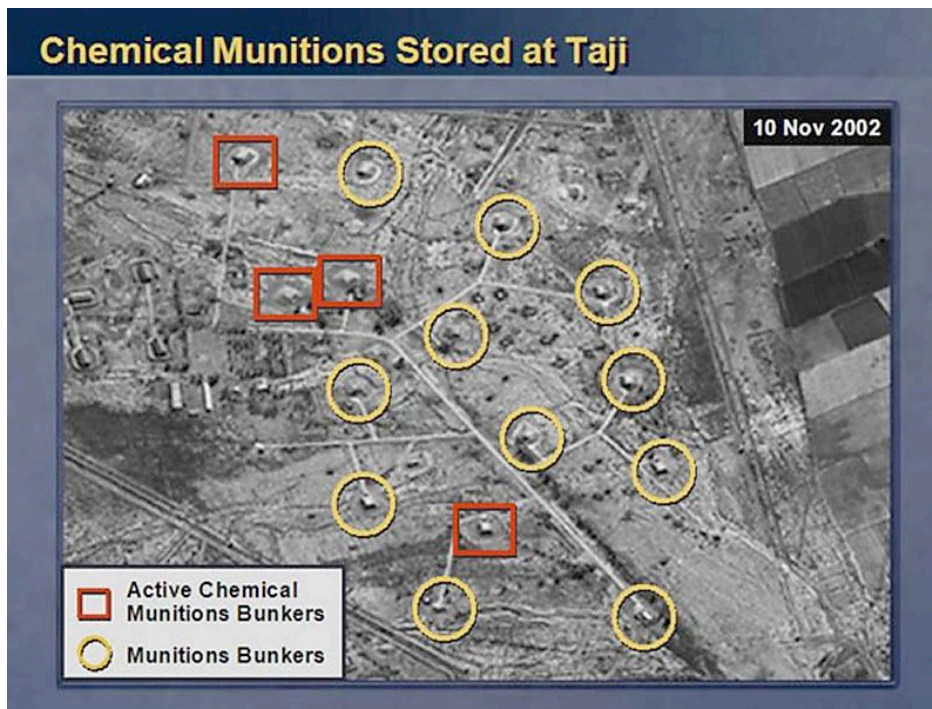


Figure 7: Iraq Weapons Sites

But the nature of the threat is even more specific in Powell's presentation:

We know from Iraq's past admissions that it has successfully weaponized not only anthrax, but also other biological agents including botulinum toxin, aflatoxin and ricin. But Iraq's research efforts did not stop there. Saddam Hussein has investigated dozens of biological agents causing diseases such as gas-gangrene, plague, typhus, tetanus, cholera, camelpox, and hemorrhagic fever. And he also has the wherewithal to develop smallpox....The Iraqi regime has also developed ways to disperse lethal biological agents widely, indiscriminately into the water supply, into the air. For example, Iraq had a program to modify aerial fuel tanks for Mirage jets. This video of an Iraqi test flight obtained by UNSCOM some years ago shows an Iraqi F-1 Mirage jet aircraft. Note the spray coming from beneath the Mirage. That is 2,000 liters of simulated anthrax that a jet is spraying. In 1995, an Iraqi military officer, Mujahid Salleh Abdul Latif told inspectors that Iraq intended the spray tanks to be mounted onto a MiG-21 that had been converted into an unmanned aerial vehicle, or UAV. UAVs outfitted with spray tanks constitute an ideal method for launching a terrorist attack using biological weapons...

*We know.* Powell here describes the variety of "weaponized" biological agents, as well as the intense interest of the Hussein regime in finding ways to deliver them. Iraqi jets as well as unmanned aerial vehicles are presented as a means not only of threatening Middle Eastern states but also the U.S. and Britain. After this discussion of WMDs, Iraqi capabilities, and interests, Powell concludes not only that the weapons inspectors have failed but that the threat is

immediate:

There can be no doubt that Saddam Hussein has biological weapons and the capability to rapidly produce more, many more. And he has the ability to dispense these lethal poisons and diseases in ways that can cause massive death and destruction.

*There can be no doubt.* Secretary of State Powell's cartoons and fuzzy pictures of industrial sites appear, in retrospect, not simply as a fabrication of knowledge but rather as a tactical deployment of the idea of secret information, for his presentation was loaded with the promise that more detailed and exacting information existed, that could not be made public without putting U.S. interests at risk. Indeed, he began his presentation by stating: "I cannot tell you everything that we know, but what I can share with you, when combined with what all of us have learned over the years, is deeply troubling."

The deployment of "secret" knowledge as political propaganda relied here on the mechanisms of government that were initially established to protect information about the U.S. nuclear arsenal. The argument for an invasion of Iraq also drew on culturally established forms of nuclear fear developed in the U.S. during the Cold War. We see here one end result of this multigenerational system of secrecy: a fundamental corruption in the terms of knowledge, where the idea of knowledge replaces actual content as a means of engaging the world. The "will to believe" (in Iraqi "wmds" and links between Saddam Hussein and Al-Qaeda) by the Bush Administration is staggering but it was only enabled as state policy by the vast deployment of secrecy to both limit debate and to discount all alternative sources of information either irrelevant or politicized. The secrecy/threat matrix has been revealed as a core tool of governmental agency in the "war on terror" but it has also been revealed to be a highly over-determined form, one that functions to fundamentally distort both expertise and knowledge. And in a security state where knowledge itself is rendered suspect, only ideology remains as the basis for action.

<sup>1</sup> In 1992, the United States voluntarily entered into a moratorium on underground nuclear testing and new nuclear weapons design work at the national laboratories (see Masco 2004). After the Bush Administration pulled out of the Antiballistic Missile Treaty in 2002, it focused on expanding the role of U.S. nuclear weapons in its security policy. The 2002 Nuclear Posture Review – the key military planning document for U.S. nuclear policy – argued for expanding the potential targets of U.S. nuclear attack as well as for renewing the test program (for excerpts see: <http://www.globalsecurity.org/wmd/library/policy/dod/npr.htm>). In fall of 2006, Lawrence Livermore and Los Alamos National Laboratories submitted their first new design for a nuclear weapon since the 1980s. The nuclear weapons complex is currently gearing up for new weapons production, as well as a continued effort to build a state-of-the-art 21<sup>st</sup> century nuclear arsenal. See, the “Reliable Replacement Warhead” DOE program site on the internet at: <http://www.nnsa.doe.gov/reliablereplacementwarhead.htm>.

<sup>2</sup> For a detailed chronology and assessment of post-9/11 changes in government secrecy and its impact on media coverage, see The Reporters Committee for Freedom of the Press 2004.

<sup>3</sup> Bush signed in 2003 Executive order 13292 – which permitted classification of “scientific, technological, or economic matter relation to the national security, which include defense against transnational terrorism,” see Knezo (2003) and Waxman (2004).

<sup>4</sup> See, OpenTheGovernment.Org 2005a and 2005b.

<sup>5</sup> See also, the National Security Archives discussion of the reclassification program at: <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB179/index.htm>.

<sup>6</sup> See, Frank Bass and Randy Herschaft “1M Archived Pages Removed Post-9/11” *Associated Press*, March 13, 2007.

<sup>7</sup> One exception is the wikipedia project, a technology that allows anybody to edit web-based entries, creating a new kind of resource drawn from collective engagements. The advantage of this technology is in collective knowledge (rather than compartmentalized knowledge), which has now been recognized by the CIA, who has constructed their own wikipedia (see, <http://en.wikipedia.org/wiki/Intellipedia>). The CIA’s Intellipedia is secret (because it is not accessible to the public) but not compartmentalized, as anyone on the CIA network can upload data or correct existing entries. A more radical use of the Wiki technology, is the Wikileaks project, which promises to create an (see, <http://wikileaks.org/>):

uncensorable Wikipedia for untraceable mass document leaking and analysis. Our primary interests are oppressive regimes in Asia, the former Soviet bloc, Sub-Saharan Africa and the Middle East, but we also expect to be of assistance to those in the West who wish to reveal unethical behavior in their own governments and corporations. Boasting over 1.2 million documents already on-line, wikileaks is an effort to recover the idea of accountability by deploying a global technology to counter official secrecy with a global counter archive of leaked materials.

<sup>8</sup> For a transcript, see: <http://www.whitehouse.gov/news/releases/2002/08/20020826.html>. Secretary of Defense Rumsfeld reiterated these claims during the first weeks of the war in an interview on ABC News, claiming that the U.S. knew exactly where the WMD where in Iraq: We know where they are. They’re in the area around Tikrit and Baghdad and east, west, south and north somewhat... I would also add, we saw from the air that there were dozens of trucks that went into that facility after the existence of it became public in the press and they moved things out. They dispersed them and took them away. So there may be nothing left. I don’t know that. But it’s way too soon to know. The exploitation is just starting. For a transcript, see: [http://www.defenselink.mil/transcripts/2003/t03302003\\_t0330sdabcsteph.html](http://www.defenselink.mil/transcripts/2003/t03302003_t0330sdabcsteph.html)

---

<sup>9</sup> For a transcript of Powell presentation to the United Nations, as well as copies of his slide presentation, see: <http://www.globalsecurity.org/wmd/library/news/iraq/2003/iraq-030205-powell-un-17300pf.htm>.

---

## References

- Ellsberg, Daniel  
 2003 *Secrets: A Memoir of Vietnam and the Pentagon Papers*. New York: Penguin.
- Foucault, Michel  
 2003 *Society Must Be Defended: Lectures at the College de France, 1975-6*. New York: Picador.  
 1995 *Discipline and Punish: The Birth of the Prison*. New York: Vintage.
- Galison, Peter  
 2004 "Removing Knowledge" *Critical Inquiry* 31.
- Knezo, Genevieve J.  
 2003 "Sensitive but Unclassified" and other Federal Security Controls of Scientific and Technical Information: History and Current Controversy. Washington: Congressional Research Service.
- Masco, Joseph  
 2006 *The Nuclear Borderlands: The Manhattan Project in Post-Cold War New Mexico*. Princeton: Princeton University Press.  
 2004 "Nuclear Technoesthetics: Sensory Politics from Trinity to the Virtual Bomb in Los Alamos" *American Ethnologist* 31(3):1-25.  
 2002 "Lie Detectors: On Secrets and Hypersecurity in Los Alamos" *Public Culture* 14(3): 441-467.
- Open The Government  
 2005a Secrecy Report Card 2005. Available on-line at" [www.OpenTheGovernment.org](http://www.OpenTheGovernment.org).  
 2005b Secrecy Report Card 2005: An Update. Available on-line at" [www.OpenTheGovernment.org](http://www.OpenTheGovernment.org)
- Pozen, David  
 2005 "The Mosaic Theory, National Security, and the Freedom of Information Act" *The Yale Law Journal* 115:628-79.
- Prados, John and Margaret Pratt Porter (eds)  
 2004 *Inside the Pentagon Papers*. Lawrence: University of Kansas Press.
- The Reporters Committee for Freedom of the Press  
 2004 *Homefront Confidential: How the War on Terrorism Affects Access to Information and the Public's Right to Know*. Available on the Internet at: [www.rcfp.org/homefrontconfidential](http://www.rcfp.org/homefrontconfidential).
- Roberts, Alasdair  
 2006 *Blacked Out: Government Secrecy in the Information Age*. Cambridge: Cambridge University Press.
- U.S. Department of Energy  
 1994 *Closing the Circle on the Splitting of the Atom*. Washington, D.C.: DOE Office of Environmental Management.

---

U.S. Government Accountability Office

- 2006 *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-related and Sensitive But Unclassified Information.* Washington: U.S. Government Accountability Office.

U.S. Information Security Oversight Office (ISOO)

- 2006 Audit Report: Withdrawal of Records from Public Access at the National Archives and Records Administration for Classification Purposes.
- 2004a Report on Cost Estimates for Security classification Activities for 2004.
- 2004b 2004 Report to the President.