Testimony of
Kenneth F. Bunting
Executive Director, National Freedom of Information Coalition
Columbia, MO

Before the U.S. Senate Committee on the Judiciary

March 13, 2012

"The Freedom of Information Act: Safeguarding Critical Infrastructure and the Public's Right to Know"

Mr. Chairman. Ranking Member Grassley. Members of the Committee. Thank you for the opportunity to be here this morning.

My name is Ken Bunting. I am executive director of the National Freedom of Information Coalition, headquartered at the University of Missouri School of Journalism in Columbia, MO. The NFOIC, the acronym by which our organization is perhaps better known, is a nonpartisan nationwide network of allied state and regional open government groups that work to promote government transparency, accountability, and access to information by citizens and journalists around the country.

I am here today, early in the annual recognition of what we call "Sunshine Week," to ask that the principles of open, accountable government not be cast aside as collateral damage as you wrestle with policy issues surrounding necessary protections for information about the nation's critical infrastructure and matters related to cybersecurity.

We recognize that there are circumstances under which some information and details about critical infrastructure, both of the physical and virtual nature, need to be shielded from full dissemination to the general public. We recognize that one of the legitimate goals of the various cybersecurity bills before this Congress is creating a private-industry comfort level that will encourage information sharing that can facilitate important protections for industry's cyber networks and the government's.

But wherever the exceptions to public access related to these matters reside in statute, we feel strongly they should include: Narrow definitions; a balancing-test consideration of the public interest in disclosure; and a time-delimited review process for revisiting how long the nondisclosure protections are needed.

Mr. Chairman, we commend you for inserting narrowing language that addressed some of those concerns when some of these same issues were addressed last December in the National Defense Authorization Act. Unfortunately, none of the measures we have seen dealing with cybersecurity has similar provisions.

Protections against threats we might face as a nation need not, and should not, include carte blanche authority for the government to withhold information under an exceedingly broad and ill-defined rubric that tosses aside, in its entirety, FOIA's ''strong presumption in favor of disclosure.''

Before I assumed my current role, I spent parts of four decades as a journalist or executive in the newspaper industry, the last 17 of those years in Washington state. I believe that most of you are aware that incidents and occurrences in Washington state have had their role in leading us to this hearing.

I am referring, of course, to the travails of a retired electrician named Glen Milner, who nine years ago tried to find out something about the potential dangers he and his neighbors faced living near Naval installations in the Puget Sound region. Mr. Milner wanted to know which neighborhoods and subdivisions in and around the coastal peninsulas and islands of Kitsap and Jefferson counties might see the greatest devastation in the event of an inadvertent explosion of ordinance stored at the Navy's Indian Island facility.

Simply put, he wanted to know if he, his family and his neighbors were at risk of being blown up. He also wanted to know if there was anything he could do to help protect himself. He wanted to be a good citizen.

As you know, the Navy refused to provide that information to Mr. Milner, using an expansive interpretation of the existing "personnel"/"internal rules and practices" exemption in FOIA -- a stretched variation of an interpretation that had come to be known over the years by the nickname

"High 2." But in a ruling handed down last March in a case that grew out of a lawsuit filed by Mr. Milner in September 2006, the U.S. Supreme Court discredited the Navy's interpretation as an inappropriate overreach.

That case has now been remanded, and Mr. Milner and his lawyers are still doing battle in the legal arena for the records he first requested them in 2003.

Mr. Milner still has not received those records. Nor have he and his attorneys been reimbursed for the enormous effort and expense they have encountered, trying to make Navy do the right thing in at least considering the interests and concerns of its civilian neighbors.

Had the Navy been willing to work with its civilian neighbors, rather than resisting disclosure and disregarding their concerns, people in nearby communities would have been better equipped to work more knowledgably with their local governments on emergency preparedness, and the Navy may well have found a greater public acceptance and understanding of its concerns.

It was impossible not to see parallels as I watched the excellent MSNBC documentary, *Semper Fi: Always Faithful*, about Sgt. Ensminger and those who worked with him to ferret out the truth regarding the toxic chemicals to which military personnel and neighbors of the Camp Lejeune Marine base in Jacksonville, NC were exposed for more than three decades. I believe you will hear shortly from Sgt. Ensminger, who can say much better than I can whether the documentary filmmakers got the facts right. But as the documentary crew portrayed it, he and his supporters clung to the fervent belief that the Marine Corps would eventually do the right thing of its own volition, as information they received revealed one shocking secret after another.

Eventually instead, they came to recognize a shameful cover-up.

The moral of this powerful story and so many others is that an informed citizenry with access to information that can hold its government accountable is the greatest incentive for our governments to do the right things. That was the intent of FOIA when it was enacted, and nothing that has happened in recent years has changed that. Nor have any technological advances.

We are certainly not belittling the concerns the legislative proposals before you seek to address. But please be leery of a broad sweep in closing off information. Access to information enhances the public safety and wellbeing. Exemptions that are too broad, too loosely defined, and give too much far-reaching, unchecked authority for government to withhold information are in no one's interest.

When cybersecurity and critical infrastructure legislation addresses public disclosure, we believe it should contain at a minimum: A tight definition of the information to be exempted; a sunset for the law itself; a sunset for the protection attached to the information; and a public-interest balancing test that allows legitimately protected information to remain protected, but information being withheld primarily to protect the government from embarrassment to be disclosed.

Under several proposals that have been put forth in the past eight months, a 1995 *Dateline NBC* report that showed thousands of the nation's dams precariously close to collapse might not have been possible. Nor likely, would the report by University of Missouri students that showed only 33 of that state's 1200 dams had the current Emergency Action Plans required by law. And, after-the-fact reporting by my old newspaper and others in Washington state -- following a tragic pipeline explosion that spilled 277,000 gallons of gasoline, blew a plume of smoke 30,000 feet into the air and killed three innocent youths -- would have been severely limited. That reporting contributed to new pipeline safety legislation in Washington state, and may have even had a causal connection to the EPA investigation that led to a seven-count criminal indictment against two pipeline companies.

If all state laws had similarly lax standards on what could be withheld, it is doubtful that the *Los Angeles Times* could have reported on lagging enforcement regarding hazardous materials stored in or near public buildings, including schools and daycare centers.

And, the effort to get the Obama administration to release EPA's list of dangerous sites where coal-ash ponds seriously threaten to inundate nearby and downstream communities would be a lost cause. Just last week, nearing the one-year anniversary of the Fukushima nuclear accident in Japan, the Nuclear Regulatory Commission released a heavily redacted report that referred to seismic and flooding hazards surrounding 35 domestic nuclear

facilities using the ridiculously non-descriptive term "Generic Issue" (followed by a number). Given new criteria for withholding, NRC's refusal to provide intelligible information to the public about safety issues, already bad, will only get worse.

Without a public interest balancing test, important data and information might be withheld in instances similar to each of the examples I just recited. With one, the wisdom of making people aware of such dangers would have to be considered -- at the very least. Without sunset provisions and a periodic review process, health and public safety information imprudently hidden from public view might remain shrouded in secrecy forever -- even in the aftermath of incidents like the decades of toxic poisonings at Camp Lejeune or the tragic explosion in Washington state.

Why a sunset provision? It is because the need for access to information of this sort only grows over time. If a problem is so pervasive and dangerous that the government, despite its best efforts, cannot fix it, the public needs to know that. Further, an informed public might be able to help.

The most cynical articulation of the worst provisions of some of the legislative proposals that have been introduced in the past eight months is that they seek to legitimize the disregard shown by the Navy that forced Mr. Milner to take his quest for information all the way to the U.S. Supreme Court; and the disregard shown by the Defense Department for high incidence of illness and death among Marine families, civilian employees and neighbors near Camp Lejeune between 1957 and 1987 – unforgiveable disregard that inspired the act of Congress named for Sgt. Ensminger's late daughter.

NFOIC has joined with OpentheGovernment.org, the Project on Government Oversight, the American Society of News Editors, and other organizations concerned with government transparency and accountability to work with members of Congress on ways to protect the public's right to know while addressing concerns over information related to critical infrastructure and cybersecurity.

In communicating our concerns to members of this Committee and others in Congress, those organizations have urged that key principles be considered in addressing this important legislation. First and foremost, the presumption of disclosure that is a bedrock principle of FOIA should not be ignored or

abandoned. In addition, we ask that the public's interest in disclosure, particularly that of those living in close proximity to hazardous critical infrastructure, be taken into account. Where there is a particularized threat that justifies limits on disclosure for unclassified information, we ask that the threat be identified, be subject to judicial review, and in some cases to public comment.

And should there be instances where it is determined that there are some supposed justifications for withholding information like the toxic contamination in Camp Lejeune water, or the safety concerns that worried Mr. Milner and his neighbors, we have asked that there be special-access consideration for those facing greatest dangers because of their geographical proximity.

I urge that you not accept anyone's view that cybersecurity and appropriate protections for critical infrastructure information pose a Hobson's choice that makes "the people's right to know" entirely expendable. Please do not accept that necessary protections for information about the nation's critical infrastructure and matters related to cybersecurity cannot be achieved to co-exist with the principles of open, accountable government. They can. And they must.

Please also be mindful that the laws in the 50 states and the District of Columbia that govern transparency and openness in those jurisdictions are in many ways emulations of federal government policy on transparency. I often hear discussions of whether the federal FOIA and its policies should trump state laws, or whether states that choose to do so are within their rights when they strive to be even more open and accountable than the examples and mandates of federal law. I believe the more states are transparent, the more they are laudably serving their citizens.

If you believe in open, accountable government and consider it important, please be mindful that any legislation you pass might have public policy implications over and beyond the issues being discussed.

If you adopt a legislative standard that gives rise to, and even encourages, far-reaching and imaginative interpretations that allow the government to keep secret anything it wants to hide from public view, you will be making bad policy. And worse, it will beget more bad policy.

Thank you again for the invitation, and for your attention, Senators. I look forward to your questions.