AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–586

THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION AND THE PUBLIC'S RIGHT TO KNOW

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

MARCH 13, 2012

Serial No. J–112–63

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

76–357 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Grassley, Hon. Chuck, a U.S. Senator from the State of Iowa	2
prepared statement	98
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	102

WITNESSES

Bunting, Kenneth F., Executive Director, National Freedom of Information Coalition, Columbia, Missouri	17
Ensminger, J.M. (Jerry), Retired marine Master Sergeant, Camp Lejeune Marine Base, Elizabethtown, North Carolina	15
Nisbet, Miriam, Director, Office of Government Information Services, National Archives and Records Administration, Washington, DC	5
Pustay, Melanie Ann, Director, Office of Information Policy, U.S. Department of Justice, Washington, DC	7
Rosenzweig, Paul, Red Branch Consulting, PLLC, Professorial Lecturer in Law, George Washington University, and Visiting Fellow, The Heritage Foundation, Washington, DC	19

QUESTIONS AND ANSWERS

Responses of Miriam Nisbet to questions submitted by Senators Grassley and Klobuchar	26
Responses of Paul Roaenzweig to questions submitted by Senators Grassley, Sheldon, Whitehouse and Klobuchar	29
Responses of Melanie Pustay to questions submitted by Senators Leahy, Cornyn, Grassley and Klobuchar	33

SUBMISSIONS FOR THE RECORD

Bunting, Kenneth F., Executive Director, National Freedom of Information Coalition, Columbia, Missouri, statement	60
Epic.org, Electronic Privacy Information Center, Washington, DC, statement	66
Ensminger, J.M. (Jerry), Retired Marine Master Sergeant, Camp Lejeune Marine Base, Elizabethtown, North Carolina, statement	77
New York Times, March 10, 2012, article	104
Nisbet, Miriam, Director, Office of Government Information Services, National Archives and Records Administration, Washington, DC:	
statement	107
April 13, 2012, letter	112
April 24, 2012, letter and attachment	114
Pustay, Melanie Ann, Director, Office of Information Policy, U.S. Department of Justice, Washington, DC, statement	119
Rosenzweig, Paul, Red Branch Consulting, PLLC, Professorial Lecturer in Law, George Washington University, and Visiting Fellow, The Heritage Foundation, Washington, DC, statement	134
Sunshine in Government Initiative, Rick Blum Coordinator; National Freedom of Information Coalition, Kenneth Bunting, Executive Director; Project on Government Oversight (POGO), Angela Canterbury, Director of Public Policy; American Society of News Editors, Kevin Goldberg, Counsel; OpenTheGovernment.org, Patrice McDermott, Executive Director; and Citizens for Responsibility and Ethics in Washington, Anne Weismann, Chief Counsel, February 16, 2012, letter	146

THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION AND THE PUBLIC'S RIGHT TO KNOW

TUESDAY, MARCH 13, 2012

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The Committee met, pursuant to notice, at 10:55 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Patrick J. Leahy, Chairman of the Committee, presiding.

Present: Senators Leahy, Whitehouse, Grassley, and Cornyn.

OPENING STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. I apologize for the late start. We had the beginning of debate on judicial nominations on the floor, the Majority and Minority Leaders and myself. I may be No. 2 in seniority for the Senate, but when I have the Majority and Minority Leaders who are there engaging in the colloquy, you tend to stay around and finish it. So I do apologize.

We are holding an important hearing on one of our most cherished open-government laws, the Freedom of Information Act.

Incidentally, I spoke to the Judicial Conference this morning at the Supreme Court and made a pitch again to open up our courts to cameras and full, instantaneous coverage. When I finished saying that, we had the chief judges of all the circuit courts there and the Chief Justice, and I said I was going to pause for the thundering applause. But, instead, I paused for the thundering silence.

In the decade since September 11th, we have had to wrestle with how best to maintain the careful balance between what is legitimate Government secrecy and the public's right to know even as new national security threats emerge. Does government secrecy have its place? Of course. We were not about to announce, for example, to the press a week before the raid on Osama bin Laden. But I worry that since September 11th there has been overuse of the secrecy stamp. It is too easy to say, well, this is secret. And it may be secret because, boy, did we screw up. And when that happens, excessive government secrecy can come at an unacceptable price: harm to the American public's interests in safety, healthy living, a clean environment, and so on.

Sunshine Week is a timely reminder that as the Congress considers how best to safeguard critical infrastructure information in

cyberspace, we have to safeguard the American public's right to know about threats to their health and safety. Last year, the Supreme Court held in *Milner* v. *Navy* that the Government could not rely upon Exemption 2 under FOIA to withhold explosives maps from the public. That was an important victory. But now in its wake, Congress is considering several new legislative exemptions to FOIA. We should do that pretty carefully.

In January, President Obama signed into law a carefully balanced, narrow exemption to FOIA for Department of Defense critical infrastructure information, and I helped craft that. It requires Government officials to affirmatively determine that withholding critical infrastructure information from the public outweighs other interests, such as ensuring that we have information that may concern our health and safety. Truly sensitive things can be withheld, but not as a knee-jerk reaction. So I intend to continue to work with other members on both sides of the aisle as we try to fulfill this goal.

I am going to put my full statement in the record, but I commend the Obama administration for taking a number of important steps to improve transparency, such as the 'ethics.gov' portal.

Senator Cornyn and I, and before him, other Republican Senators, have done a lot of the legislation on FOIA. It should not be a partisan issue because I do not care whether you have a Democratic or Republican administration, there is always going to be some who are going to want to say, "Why do we have to release this information?" Well, my response would be, "Because you represent all Americans, and we have a right to it."

[The prepared statement of Chairman Leahy appears as a submission for the record.]

Chairman LEAHY. Senator Grassley.

STATEMENT OF HON. CHUCK GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Senator GRASSLEY. Mr. President—or, Mr. Chairman, before——

[Laughter.]

Senator GRASSLEY. That was a slip. I was not trying to be——

Chairman LEAHY. I must admit that I am one of the very few Senators who has never had the desire to be President. Go ahead.

Senator GRASSLEY. Before I read, I agree with what you have said except one little part, and I think I will preface my remarks with this: You know, I do not care whether we have a Republican or Democrat President, it is very, very difficult not only under FOIA but under our constitutional responsibility of oversight to get information. It is just a culture in the executive branch that is difficult to overcome. And the only reason I would separate out President Obama a little bit different from others is, as you said, he has put in place some statements and policies that are for more transparency and more openness. But I find it difficult, if I measure what he said he wanted to do, with what has actually materialized as either he did not mean it or—and I think he did mean it—and, No. 2, the people below him are not carrying out his policies.

So I thank you for holding this hearing. Open government and transparency are essential for our democratic form of government. And I think James Madison had something very good to say about

this: "a people who mean to be their own Governors must arm themselves with the power which knowledge gives." And, of course, that knowledge comes from knowing what is going on in our Government, among other things.

The Freedom of Information Act codifies this fundamental principle which our Founders found so valuable. So it is important to talk about the Act and the need for American citizens to be able to obtain information about how their Government is operating.

Although it is Sunshine Week, I am sorry to report that, contrary to the President's proclamations when he took office, after 3 years I do not believe the sun is shining commensurate with his statements that he wanted to be the most transparent of any administration in history.

Based upon my experience in trying to pry information from the executive branch, I am disappointed to report that agencies under the control of President Obama's political appointees have been more aggressive than ever in withholding information from the public and Congress.

There is a complete disconnect between the President's grand pronouncements about transparency and the actions of his political appointees.

On his first full day in office, the President issued a memorandum on FOIA. In it, he wrote that Executive agencies should "adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open government." All you can say to that is, "Amen."

But, unfortunately, it appears that in the eyes of the President's political appointees—and maybe for this the President has a big, big job, maybe he cannot keep track of what everybody does or the trends in his administration—but his proclamations about open government and transparency are being ignored.

Indeed, FOIA requesters appear to have reached the same conclusion. I will give you an example. When recently asked about President Obama and FOIA, Katherine Meyer, an attorney who has been filing FOIA cases since 1978, said, that the Obama administration "is the worst on FOIA issues. The worst. There is just no question about it. This administration is raising one barrier after another. It has gotten to the point where I am stunned. I am really stunned."

The problem is more than just a matter of backlogs with answering FOIA requests. Based on investigative reports, we have learned of inappropriate actions by the President's political appointees.

In March of last year, 2 weeks after this Committee held a hearing on FOIA, the House Committee on Oversight and Government Reform released a 153-page report on its investigation of the political vetting of FOIA requests by the Department of Homeland Security. The Committee reviewed thousands of pages of internal e-mails and memoranda and conducted six transcribed interviews.

The Committee, under Chairman Issa, learned that political staff under the Secretary of Homeland Security corrupted the agency's FOIA compliance procedures, exerted pressure on FOIA compliance officers, and undermined the Federal Government's accountability to the American people. The report's findings are disturbing, and I will just summarize four of them.

First, the report finds that by the end of September 2009, copies of all significant FOIA requests had to be forwarded to Secretary Napolitano's political staff for review. The career staff in the FOIA office were not permitted to release responses to these requests without approval from political staff.

Second, career FOIA professionals were burdened by the intrusive political staff and blamed for delays, mistakes, and inefficiencies for which the Secretary's political staff was responsible. The Chief Privacy Officer, herself a political appointee, did not adequately support and defend career staff. To the contrary, in one of her e-mails, she referred to her career staff as "idiots."

Third, political appointees displayed hostility toward career staff. In one e-mail, political staff referred to a senior career FOIA employee as a "lunatic" and wrote of attending a FOIA training session organized by the career staffer for the "comic relief." Moreover, three of the four career staff interviewed by the Committee have been transferred, demoted, or relieved of certain responsibilities.

Last, the report finds that the Secretary's office and the General Counsel's office can still withhold and delay significant responses. Although the FOIA office no longer needs an affirmative statement of approval, the Secretary's political staff retains the ability to halt the release of FOIA responses.

The conduct of the political appointees at Homeland Security involved the politically motivated withholding of information about the very conduct of our Government from our citizens. In particular, it was the withholding of information about the administration's controversial policies and about its mistakes. That was a direct violation of the President's orders.

I am disappointed that there was not more coverage of Chairman Issa's report and the inappropriate conduct by political appointees at Homeland Security. I am also disappointed that the Justice Department has not conducted an investigation of this scandal.

I have to say that I am a bit surprised that some open-government and privacy groups appear to be accepting the dramatic regulatory power that Homeland Security and Secretary Napolitano will have under the Lieberman-Collins cybersecurity bill and under President Obama's proposal. Given the FOIA scandal at Homeland Security, I would have thought that they would have more reservations.

I am also sorry to say that the Department of Homeland Security is not alone when it comes to questionable actions. Recently, the National Security Archive gave its annual Rosemary Award to the Department of Justice for the worst open-government performance in 2011.

The charges the Archive makes against the Justice Department include:

One, proposing regulations that would allow the Government to lie about the existence of records sought by FOIA requesters, and that would further limit requesters' ability to obtain information;

Two, using recycled legal arguments for greater secrecy, including questionable arguments before the Supreme Court in 2011 in direct contradiction to President Obama's presumption of openness;

And, three, backsliding on the key indicator of the most discretionary FOIA exemption, Exemption 5 for deliberative process. In

2011, the Justice Department cited Exemption 5 to withhold information 1,500 times, and that is up from 1,231 times in 2010.

According to the Archive, the Justice Department edged out a crowded field of contending agencies that seem to be in "practical rebellion" against President Obama's open-government orders.

So there is a disturbing contradiction between President Obama's grand pronouncements and the actions of his political appointees. The Obama administration does not understand that open government and transparency must be about more than just pleasant sounding words in memos. Ultimately, the President is responsible for the conduct of his political appointees, especially after 3 years in office. And both he and Attorney General Holder certainly know what is going on.

Throughout my career I have been actively conducting oversight of the executive branch regardless of who controls the Congress or the White House. Open government is not a Republican or a Democrat issue. It has to be a bipartisan issue. It is about basic good government and accountability—not party politics or ideology.

I started out my remarks by quoting James Madison. Madison understood the danger posed by the type of conduct we see in a lot of administrations, but this one has not lived up to what they said that they intended to do. He explained that "[a] popular government without popular information or the means of acquiring it, is but a prologue to a farce, or a tragedy, or perhaps both."

So I am looking forward to hearing the testimony. I want to thank all the witnesses for coming in today, and taking time.

I also want to thank Sergeant Ensminger for his service to our country. I am very sorry about the loss of his daughter. I am also cosponsoring the Caring for Camp Lejeune Veterans Act, and this was brought to my attention about 4 years ago. People in my constituency that I did not even know existed came to my town meetings and came to Iowa. They were very much injured by what happened at Camp Lejeune, and I thank them for bringing that to my attention. And they were not leading a very high quality of life.

Thank you, Mr. Chairman.

Chairman LEAHY. Thank you.

Our first witness is Melanie Pustay, who is the Director of the Office of Information Policy at the Department of Justice.

I am sorry. Actually, our first witness is Miriam Nisbet, the Director of the Office of Government Information Services at the National Archives. She served as the Director of the Information Society Division for UNESCO in Paris. She earned her bachelor's degree and law degree from the University of North Carolina.

I appreciate having you here. I apologize for my voice. It worked fine in Vermont yesterday. I got off the airplane yesterday and found that we have a few more pollens in the air than snow-covered Vermont. Go ahead, Dr. Nisbet.

STATEMENT OF MIRIAM NISBET, DIRECTOR, OFFICE OF GOVERNMENT INFORMATION SERVICES, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, WASHINGTON, DC

Ms. NISBET. Thank you, Mr. Chairman, Senator Grassley. Thank you for having me this morning. And, yes, I can feel that pollen a little bit, too, so bear with me, please.

As both of you have mentioned this morning, the Freedom of Information Act is a cornerstone of our democracy, and we at the National Archives are proud to display the original Freedom of Information Act in the Rotunda of the Archives this week during Sunshine Week. For the first time, it is being displayed, and we would like to invite you to come and visit us.

An important part of the Freedom of Information Act is protecting sensitive information even as the Government strives to give the public the greatest access to records under the law.

I am here to provide you with a sense of what we are hearing from requesters and agencies about safeguarding critical infrastructure information and other records previously protected under Exemption 2 of the FOIA. In our work at the Office of Government Information Services, or OGIS, as the FOIA ombudsman, we talk every day with agency FOIA professionals and FOIA requesters. In fact, we have worked with requesters and agencies on more than 1,500 specific matters since we opened in September 2009. When Congress created OGIS as part of FOIA, the statutory mandate for our office included working to improve the FOIA process. We do that as we fulfill our two-pronged mission: reviewing agency FOIA policies, procedures, and compliance, which allows us to see how agencies carry out the law; and working to resolve FOIA disputes between agencies and requesters, which shows us where there are trouble spots. We regularly meet with and hear from requesters and agency professionals to discuss trends, problems, complaints, and improvements to FOIA's implementation.

Chairman LEAHY. Dr. Nisbet, we have all this and your whole statement is part of the record, but if you could direct us to which agencies are actually complying with FOIA as they should, which ones are not, and why.

Ms. NISBET. I would be happy to do that, and if I could, let me supplement the record with information about that. In fact, we are releasing a report on our activities for fiscal year 2011 this week, Mr. Chairman, and there will be a great deal of information about precisely what we have seen.

Chairman LEAHY. Which agency does the best job and which does the worst?

Ms. NISBET. I do feel like I am in the hot seat. I would say that there are a number of agencies that we have seen that are working very hard. We see that every day. The Department of the Interior, for example, is one that we have worked with. Not only has it been working on improving its FOIA process overall, but it has begun working with us to train its FOIA professionals in dispute resolution skills in order to help them do their job better and to carry out the FOIA in a very collaborative way that would avoid litigation. So I think that is really a good example.

Chairman LEAHY. Which ones are the worst? You are the expert.

Ms. NISBET. I think there are a number of agencies that are still working very hard with overcoming their backlog problems, and that is in some part due to resources. That is a perennial problem, as you know. And I really would prefer not to get too much into detail about the ones that are not doing a good job.

Senator GRASSLEY. Just remember, you are not elected. We are elected. We can get in trouble for answering that question. You cannot get in trouble.

[Laughter.]

Ms. NISBET. I do not know about that, Senator Grassley.

Chairman LEAHY. Thank you.

[The prepared statement of Ms. Nisbet appears as a submission for the record.]

Chairman LEAHY. Ms. Pustay is Director of the Office of Information Policy, OIP, at the Department of Justice. Before becoming the office's Director, she served for 8 years as Deputy Director. She earned her law degree from American University's Washington College of Law where she served on law review, and disregard her B.A. from George Mason.

Again, I apologize for the voice. Please go ahead.

STATEMENT OF MELANIE ANN PUSTAY, DIRECTOR, OFFICE OF INFORMATION POLICY, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Ms. PUSTAY. No problem. Thank you. Good afternoon, Chairman Leahy and Ranking Member Grassley and members of the Committee. I am pleased to be here during Sunshine Week to address the effect of the Supreme Court's decision in *Milner* v. *Department of the Navy* and also to discuss the Department of Justice's continuing efforts to ensure that President Obama's Memorandum on the FOIA, as well as Attorney General Holder's FOIA Guidelines, are fully implemented.

As you know, the Attorney General issued his new FOIA Guidelines during Sunshine Week 3 years ago, and based on our review of the Chief FOIA Officer reports and agency annual FOIA reports, it is clear to us that agencies are continuing to make significant, tangible progress in implementing the guidelines.

In fiscal year 2011, despite being faced with a noticeable increase in the number of incoming requests, agencies overall were able to process over 30,000 more requests than last fiscal year. And, most significantly, when agencies processed those requests, they increased the amount of material they provided. The Government released records in response to 93 percent of requests where records were located and processed for disclosure. This marks the third straight year we have had such a significantly high release rate.

Agencies are also continuing to meet the demand for information by proactively posting information of interest to the public on their websites. Many agencies have taken steps to make the information on their websites more useful to the public by redesigning the websites, adding enhanced search capabilities, utilizing online portals and dashboards.

I am also pleased to report in particular on the successes achieved by the Department of Justice. This past fiscal year, the Department increased the number of responses to requests where records were released, and for the second straight year, we maintained a record high release rate of 94 percent for all requests involving responsive records that were processed for disclosure.

And perhaps even more significantly, of those requests we released records in full 79 percent, which means that the requester got everything they asked for with no excisions.

Despite 3 straight years of receiving over 60,000 requests, the Department reduced its backlog of pending requests by 26 percent. We also improved the average processing time for simple and complex requests.

Now, my office also carries out the Department's statutory responsibility to encourage compliance with the FOIA. And, of course, this guidance was particularly needed in the wake of the dramatic narrowing of Exemption 2 that occurred when the Supreme Court issued its opinion in *Milner*.

As you know, in *Milner*, the Supreme Court overturned 30 years of established FOIA precedent by restricting the scope of Exemption 2 to matters that relate solely to personnel rules and practices. Prior to *Milner*, agencies had long followed the interpretation of Exemption 2 provided by the D.C. Circuit, which applied a two-part test that was announced in the *Crooker* case. Under *Crooker*, information first had to qualify as "predominantly internal" and, second, it had to be either of no public interest, which was referred to as "Low 2," or be more substantial in nature where disclosure would risk circumvention of the law, and that was referred to as "High 2." We had a substantial body of case law developed over the years concerning High 2, with courts upholding protection for many different types of sensitive information when disclosure would risk circumvention of the law. But as a result of the Supreme Court's rejection of High 2 as inconsistent with the plain language of the exemption, there is a wide range of sensitive material whose disclosure could cause harm and which had previously been protected and which is now at risk.

The Supreme Court was sympathetic in its decision to the policy concerns raised by the Government regarding the need to protect information when its disclosure risked harm. And the Court even acknowledged that it might be necessary for the Government to seek relief from Congress.

Now, in the months since the *Milner* decision, some agencies have sought statutory relief under the FOIA for discrete categories of information. However, this piecemeal approach does not sufficiently ensure protection for all agencies and for all categories of information that were long protected under High 2. And we believe that the preferred course of action would be to amend Exemption 2 so that its plain language addresses the need to protect against disclosure where that disclosure would risk circumvention of the law.

Open-government groups, reporters, and other interested members of the FOIA requester community are understandably interested in this issue as well, and the precise contours of a legislative amendment to Exemption 2 will need to take into account both the interests of the agencies in making sure that there is no circumvention of the law and the interests of the requesters and open-government groups in ensuring that exemptions are precisely crafted so as not to unnecessarily sweep too broadly.

In closing, the Department of Justice looks forward to working together with the Committee on all matters pertaining to the gov-

ernmentwide administration of the FOIA, including efforts to address the effect of the *Milner* decision.

[The prepared statement of Ms. Pustay appears as a submission for the record.]

Chairman LEAHY. Well, thank you. You have mentioned the *Milner* case; what guidance is DOJ giving to agencies about how they should respond, and how they should treat FOIA requests seeking critical infrastructure information?

Ms. PUSTAY. In the wake of the Supreme Court's decision, we issued extensive guidance to agencies to help walk them through the changed landscape that occurred as a result of the Supreme Court's decision. First of all, of course, we had to explain what Exemption 2—what was left of the exemption—covered and what would fit within it. But pragmatically, because High 2 is now no longer a part of the protection afforded by Exemption 2, agencies really have two alternatives: to try to see if other exemptions will safeguard the information, and that is certainly an option that was discussed and contemplated in the *Milner* case itself, the information that——

Chairman LEAHY. Of course, in the National Defense Act, we tried to put in a very, very narrow exemption.

Ms. PUSTAY. Exactly. And the other alternative, if existing exemptions do not cover the information—let me actually first say, as part of our guidance, we instructed agencies to first consider whether or not the information needed to be protected. We made a point of highlighting the Attorney General's FOIA guidelines and the presumption of openness, and we always make sure that we use that as our starting point before we even get to the point of protecting. But assuming there is risk of circumvention, if existing FOIA exemptions——

Chairman LEAHY. It was too easily used before.

Ms. PUSTAY. Right now the alternatives would be using other FOIA exemptions or seeking relief through specific statutory provisions that are covered under Exemption 3.

Chairman LEAHY. Dr. Nisbet, how do you see agencies handling these requests for critical infrastructure information? Are they following the *Milner* decision?

Ms. NISBET. Well, of course, they are following the *Milner* decision, and they are using language that the Supreme Court used to suggest to them that they do look for other exemptions. And in some cases, that certainly does work. But it does not work in all cases.

For example, Exemption 7, which applies to records or information compiled for law enforcement information, certainly could apply to certain sensitive information, particularly as it relates to security measures or preventing crime. But Exemption 7 is not available to all agencies.

Similarly, Exemption 1 would not be a good choice. Certainly, some agencies do not have classification authority nor, as this Committee has recognized, is expanding the universe of classified information something that we want to see.

Chairman LEAHY. Also, back in 2007, Senator Cornyn and I authored the Open Government Act to strengthen FOIA, and in it we have the Office of Government Information Services regularly re-

porting to Congress on recommendations to improve FOIA compliance within the Government. We have not seen those reports. What is the current status of the reports that the law requires?

Ms. NISBET. Let me distinguish between reporting on our activity, which we have done and we have made public——

Chairman LEAHY. I am talking about the report that is required to be made to Congress on recommendations to improve FOIA compliance within the Government.

Ms. NISBET. Yes, Mr. Chairman, as to recommendations which we have put through the process for review with OMB, we have——

Chairman LEAHY. When did you put it through the process to be reviewed?

Ms. NISBET. Well, the first set of recommendations were given just a little over a year ago. Those did get held up. I am not sure that I can explain why. But I can tell you that we are working with OMB now to get that process going on.

Chairman LEAHY. Recommendations were made over a year ago, and we have not received them yet. The law requires us to receive them. When will we receive them?

Ms. NISBET. I hope you will receive something very shortly. However, I will tell you that we are working with OMB actively to see whether or not some of the suggestions that we had might be able to be addressed administratively without asking Congress to make any legislative changes.

Chairman LEAHY. Well——

Senator GRASSLEY. Mr. Chairman, what I would like to know is: Is it her fault or OMB's fault that they are not——

Chairman LEAHY. The law is pretty clear about us getting the reports. We have not gotten the reports. Who is at fault?

Senator GRASSLEY. We run into this. Just recently, with an agricultural rule, they studied it for 2 years, and it was sitting in OMB. Finally, after we wrote a letter, OMB released it.

Chairman LEAHY. So my question is: Who is not following the law?

Ms. NISBET. Well, one question I might ask you, Mr. Chairman, is the law does not state how often these recommendations need to be made.

Chairman LEAHY. I think if the recommendations were made a year ago, even if mail has been kind of slow—I mean, I am happy to drive down there and pick it up if that would speed things up.

[Laughter.]

Chairman LEAHY. You know, I would be happy to, if they would let me in the building.

Ms. NISBET. Thank you, Mr. Chairman.

Chairman LEAHY. When will we get it?

Ms. NISBET. I will have something to you—how about within a month we will have something? I will work actively with OMB to make that happen.

Chairman LEAHY. Tell them at OMB that this is not a partisan thing. Both Senator Grassley and I would kind of like to hear from them. I know they are very busy, but——

Senator GRASSLEY. Would it help you if we would write a letter to OMB and tell them to get off the pot?

Ms. NISBET. I think your statements here today will really say what you mean.

Chairman LEAHY. You know, I just would like to have people be happy to respond to us rather than having to subpoena things.

Ms. NISBET. Thank you.

Chairman LEAHY. We do have that alternative.

OK. Earlier this year, the National Archives and Records Administration, the Environmental Protection Agency, and the Department of Commerce announced the creation of a multi-agency FOIA portal that automates FOIA processing, stores FOIA requests, and responds in electronic format. If it works as it should, it would make it easier for FOIA requesters. Does the Department of Justice support this kind of a FOIA portal concept?

Ms. PUSTAY. Yes, we absolutely do. The EPA is launching a pilot to build on those capabilities. What I think is important and what you will be happy to hear is that we have over 100 different offices across the Government that already have online request capability. We do think it is an important improvement to FOIA. And just this week, my office—actually, the Attorney General announced this yesterday at our Sunshine Week event—that we have an online portal for the senior management offices of the Justice Department. So requesters can go online at the website in my office, set up a personal account, make their request online, be able to track the status of their request online any time day or night, and to get their responsive documents back through the portal.

Chairman LEAHY. Of course, that is an easier way. I have a 6-year-old grandson who showed me how he goes online, although I am telling him not to go on Google because they now have a new plan to spy on Americans. That is just a personal concept.

Senator Grassley.

Senator GRASSLEY. Thank you, Mr. Chairman. And if I can help you in any way, make sure that you call on me on that request.

Ms. PUSTAY. We still accept requests the old-fashioned way as well, Senator Leahy.

Senator GRASSLEY. My first question is going to be asked for Senator Cornyn because he was here for a while but had to go to a meeting at 11. It is to Ms. Pustay. A March 9th article in Atlanticwire.com raises questions about the way the Justice Department is actually calculating reporting "backlogs" and "pending requests." How do you explain the almost 50-percent discrepancy between claimed backlogs, 3,816, and the pending requests, 6,897? Now, Senator Cornyn says, "I can understand not counting a few pending requests at the end of the year as backlog, especially if the statutory deadlines have not run. But I cannot imagine that you received 3,000 new requests at the end of fiscal year 2011 that fit that criteria. Could you explain the standards and definitions that are applied? And then, more importantly, isn't it appropriate to treat all requests alike for backlog purposes once the agency's response is overdue?"

Ms. PUSTAY. I am happy to address that question. There is a difference between pending and backlogged. Pending just means a request is open at the moment that the fiscal year closes on September 30th. Backlogged means it has been pending beyond the statutory time period.

The FOIA itself actually requires agencies to report the number of requests that are pending. The Department of Justice added the requirement that agencies report the number of requests that are backlogged because we think it is a more accurate measurement to know not just how many requests came in literally on September 30th, but how many of those requests were backlogged. So that is why we track both statistics, backlog and pending.

But we get at the Department of Justice 5,000 requests every single month, so having numbers of 3,000 and 5,000 as our pending and backlog is totally logical. We get 5,000 requests every single month.

Senator GRASSLEY. I would ask you for myself, Ms. Pustay, the National Security Archives recently gave the Rosemary Award to Justice for the worst open-government performance last year. As part of the award, the Archive stated that you presided over the development of a series of proposed regulations that would have changed the FOIA process in more than a dozen regressive ways. A two-part question, and I will ask both of them.

First, what is your response to the Archive's citing of the Justice Department as having this performance record?

And, second, what is your response to the Archive's statement about the proposed FOIA regressive regulations?

Ms. PUSTAY. I will take it in reverse order. The regulation comment is very straightforward. Our regulations were—the changes that we made were simply designed to streamline, simplify, and update the regulations. The comments that we received showed that people misinterpreted what we were trying to do, misconstrued some of the provisions, and also did not necessarily understand the fee guidelines that govern the fee categories that are put out by—that are governed by OMB's fee guidelines. So all of those issues regarding the regulations, we are happy to have the comments because we can now explain, walk requesters through, walk the public through, what we were intending to do with our regulations. So the comment period itself I think will clear that up very easily.

As to my overall reaction, of course, I am happy to be able to stand by our record at the Department of Justice. I am very proud of our record. We passed out before the hearing a list of our accomplishments to all the members, and I think it is a really stellar example of the work that has been done by the Justice Department. We have reduced our backlogs. We released—79 percent of requests got a full release of information. Our release rate for 2 years in a row is 94.5 percent, which means that requesters who come to the Department of Justice and ask for information are getting information 94.5 percent of the time. We have also done a lot of work with proactive disclosures, making more information available on our website. We have worked with agencies to try to help spread the word of transparency, to help further implement the Attorney General's guidelines. We have built FOIA.gov, a brand-new website that breathes life into all the dry FOIA statistics and lets them be interactable and much more accessible to the public.

So I can go on and on. I feel like we have a really strong record, and I stand by it.

Senator GRASSLEY. After Senator Whitehouse gets done, I would like to ask for another 5 minutes, if I could.

Chairman LEAHY. Yes, but the vote is coming up. We are going to have to keep it short because otherwise, we are not going to get the other panel in.

Dr. Nisbet, I should note that my concern—and I hope you realize both my concern and Senator Grassley's are directed at OMB, not at you. We are trying to give you a little [clicking sound, swings hand].

[Laughter.]

Chairman LEAHY. It is going to be great to see how that is reported in the record.

[Laughter.]

Chairman LEAHY. Senator Whitehouse.

Senator WHITEHOUSE. T-L-O-C-K, perhaps? Who knows?

I am interested in the manner in which the FOIA requests can be aggregated across the system and the FOIA data can be centralized across the system. For a long time, FOIA requests have been agency by agency, and for a long time, FOIA answers are sent out and then they kind of disappear, and if somebody asks the same question later, particularly if it is to another agency, it goes back and it gets re-created.

I think it is important that there be a central FOIA request, you know, portal that people can go to. I think it is important that there be a central FOIA data base so that once something has been disclosed under FOIA, you can go and find it again and it is searchable and it is a resource. You have got the FOIA module coming along. It is kind of a pilot in that direction. Could you let me know a little bit the status of that and what you expect—give me a couple of benchmarks that you are looking for in the near future to show the success of that and the commitment to that.

Ms. PUSTAY. What I can tell you first on FOIA.gov—and then you could talk about the portal.

Ms. NISBET. Yes.

Ms. PUSTAY. FOIA.gov, which is our governmentwide website, which is designed to be a one-stop shop for FOIA, we added several things just this past year to help meet the concerns or the interests that you are expressing. For one thing, we have a find function, a search function that we put on FOIA.gov, the website, which allows an interested member of the public to enter a search term. If they are interested in Al Capone or the BP oil spill, they can put that search term into FOIA.gov. It launches a search across all agency websites. So everything that an agency has posted to date, not just their responses to FOIA requests but everything they have posted, would be captured by this search. That is particularly important because we are encouraging agencies to make proactive disclosures of information, to put things on their website separate and apart from FOIA requests. And we want the public to have access to all that information. So the find button is what is designed to help you locate information and maybe not even have to make a FOIA request.

In terms of the online capability to make requests, as I said, we have got over 100 offices that have that capability so far. Many others are working on developing them. What we did, again on

FOIA.gov to facilitate access to those portals was we now have hyperlinks to all those portals so that when you are on FOIA.gov and you decide you want to make a request to the National—well, let us pick an agency that has it, our office, or Treasury has an online request portal, or NASA, you can go right from FOIA.gov and get right in, onto their online request form.

So we have taken steps right now to make that happen, and then we are going to continue to add those functionalities to FOIA.gov as we go forward.

Senator WHITEHOUSE. And how is the module coming, Dr. Nisbet?

Ms. NISBET. The FOIA module is a project that is being run jointly by—under the lead of the Environmental Protection Agency, but with the Department of Commerce and with the National Archives as partners. It is being built right now with input from FOIA professionals throughout the Government and from requesters and is due to launch October 1st. And it will be indeed a one-stop shop. In the beginning, of course, we do not have all agencies participating, but it is going to be something Version 1 can easily be moved into Version 2 as other agencies want to join, and it would be both a place where a requester can come to one place, make a request to one agency or many agencies or all agencies, and that will at the end also provide access to any records that have been disclosed under FOIA. So we think it has a lot of promise and cost savings for the Government as well as a collaborative effort and good for requesters as well.

Senator WHITEHOUSE. Good. Well, we look forward to October 1st, and I thank the Chairman and the Ranking Member who have both over many years shown intense interest in making sure that the American people have access to these public records, and today's hearing is another example of their commitment.

Chairman LEAHY. Thank you very much.

Senator GRASSLEY. One question?

Chairman LEAHY. You have one question? Go ahead.

Senator GRASSLEY. Ms. Pustay, I want to refer to the *Milner* case. It was released more than a year ago. Some believe that the impact of the decision will be to endanger public safety. The Justice Department has not approached me or my staff about legislation to address the impact of the decision, so maybe you could tell me why the Justice Department has not submitted a legislative proposal. If, in fact, there is a threat to public safety, as people indicate, isn't it irresponsible to ignore the problem?

Ms. PUSTAY. We are actively working and look forward to continuing to work to with this Committee on the issue. As I said, the impact of *Milner* is quite significant. The Supreme Court really dramatically limited the scope of protection that had previously been afforded. And since the time of the decision, we have certainly had legislative assistance from you all in terms of protecting discrete categories of information.

As I said in my testimony, though, I think the next step is to go beyond a piecemeal approach and to work on a more comprehensive approach to the problem.

Senator GRASSLEY. I will have written questions for the record.

Chairman LEAHY. Thank you. We will have further questions. I thank you both for being here.

[The questions appears under questions and answers.]

Chairman LEAHY. Good morning. The first witness will be Jerry Ensminger. He is the public face of what may be one of the worst drinking water contamination cases in U.S. history. This retired Marine gunnery sergeant lost his 9-year-old daughter, Janey, to leukemia in 1985, taken by what Gunnery Sergeant Ensminger and many others believe was tainted water at Camp Lejeune, the base where she was conceived.

I might say parenthetically, my son, Lance Corporal Mark Patrick Leahy, also went through Camp Lejeune, and it raises even more the personal stakes. Then I read the terrible things that you went through. Mr. Ensminger retired from the military 13 years ago. He has traveled the country raising public awareness about this issue. I say retired Marine. There are no ex-Marines, as you know. Gunnery Sergeant, I am glad you are here, so please go ahead, sir.

STATEMENT OF J.M. (JERRY) ENSMINGER, RETIRED MARINE MASTER SERGEANT, CAMP LEJEUNE MARINE BASE, ELIZABETHTOWN, NC

Sergeant ENSMINGER. Thank you, Mr. Chairman.

Just to set the record straight, somebody demoted me. I am a retired master sergeant.

[Laughter.]

Chairman LEAHY. I apologize for that. Please do not tell that former lance corporal, or I would be in really deep trouble. I had heard it both ways, and I do apologize. Either way, I am darn glad you are here.

Sergeant ENSMINGER. Yes, sir, thank you.

Good morning. I would like to take the opportunity to thank the Chairman and Ranking Member for offering me this opportunity to appear here today. I am here to testify on why access to information through the Freedom of Information Act matters to me and others from Camp Lejeune and about the extreme secrecy we have encountered in trying to expose the truth.

My name is Jerry Ensminger, and I served my country faithfully for 24 years in the United States Marine Corps. My daughter Janey, the only one of my four children to either be conceived, carried or born while living aboard Camp Lejeune, was diagnosed with leukemia in 1983 at the age of 6. Janey went through hell, and all of us who loved her went through hell with her. I watched my daughter die a little bit at a time for nearly 2½ years before she finally lost her fight. The leukemia won. Janey died on 24 September 1985.

Shortly after Janey's diagnosis, I began to wonder why. Why was she stricken with this disease? I researched mine and her mother's family histories, and I could find no other child that had been diagnosed with leukemia or any other type of cancer. It was not until August 1997, 3 years after I had retired from the Marine Corps, that I heard of a report indicating that the drinking water at Camp Lejeune had been contaminated during the time that we had lived there with chemicals suspected of causing childhood cancers and

birth defects. That was the beginning of my journey on a search for answers and the truth. Little did I realize how difficult it would be getting the truth out of an organization which supposedly prides itself on honor and integrity.

None of what I am about to say is speculation. It is all facts which are borne out by the Department of the Navy and United States Marine Corps' own documents. Throughout the history of this situation and to this very day, representatives of the Department of the Navy and Marine Corps have knowingly provided investigating or studying agencies with incorrect data, they have omitted data, they have obfuscated facts and told many half-truths and total lies.

The Department of the Navy and the Marine Corps' last attempt to block the truth and foil justice is being done by redefining key information being utilized by the Agency for Toxic Substances and Disease Registry in their study reports concerning the base's contaminated tap water as critical infrastructure information, or CII. They just recently slapped a label of "For Official Use Only," or FOUO, on all documents relating to the contamination. Most of these documents and information they are labeling CII have been in the public domain for more than a decade and some for nearly 50 years. Mr. Chairman, the ATSDR estimates that as many as 1 million people were exposed to horrendous levels of carcinogenic chemicals through their drinking water at Camp Lejeune. These people need the uncensored truth concerning their exposures so they can be more vigilant about their and their family's health.

The most recent attempt by the Department of the Navy and Marine Corps to suppress the public's knowledge regarding ATSDR's Camp Lejeune studies came on 5 January of this year in the form of a letter from the Marine Corps to ATSDR. Without any public interest balancing test having been executed, key information was redacted from a critical report which experts are now saying will greatly diminish its scientific value or credibility. This was labeled CII by the Department of the Navy and Marine Corps, but the legal justifications that they cited for requesting these redactions were dubious at best. They notably did not mention the new law now governing what ultimately can be withheld from the public under the Freedom of Information Act by DOD to protect CII.

It has also been reported that the ATSDR, at the behest of the Marine Corps, is currently scrubbing their Camp Lejeune website of key data and information published in previously released reports. This is all being done without any consideration of the public's need, interest, or right to know. For many of the exposed Camp Lejeune population, this information could literally mean life or death.

Mr. Chairman, the last thing we need is more secrecy disguised as a concern for security of critical infrastructure. Any exemption must be very narrowly defined as it is in the new CII FOIA exemption for DOD. There must be an enforced public interest balancing test to ensure that any security interests outweigh other public interests, like health and safety—and there must be adequate reporting and oversight on how the exemption is used.

I want to thank Chairman Leahy and Representative Maloney for narrowing the blanket exemption to FOIA for critical infrastruc-

ture information that DOD was seeking in the NDAA for fiscal year 2012. Now all we need is oversight to ensure the law is implemented and followed. The hearing today is a good start.

Thank you.

[The prepared statement of Sergeant Ensminger appears as a submission for the record.]

Chairman LEAHY. Well, thank you, Sergeant. And let me tell you, I will carry my interest in this matter beyond this hearing. We Vermonters are sometimes known as being pretty tenacious, and I will be. And I will not demote you next time, I apologize.

[Laughter.]

Sergeant ENSMINGER. That is all right, sir.

Chairman LEAHY. Thank you very much.

Our next witness is Kenneth Bunting, the first full-time executive director of the National Freedom of Information Coalition created in 2010. Before joining that, he spent parts of four decades as a journalist and newspaper industry leader, and ranking editor of the Seattle Post Intelligencer, which during that time won more national and regional awards for journalistic excellence than at any other time in its 146-year history, including the Pulitzer in 1999 and 2003. Congratulations. He has his B.S. from Texas Christian University.

Mr. Bunting, we are delighted to have you here, and I am stepping out for a moment while you testify, and that is not from a lack of interest, I can assure you. Senator Grassley will be here. I have read your testimony, and I will be back.

STATEMENT OF KENNETH F. BUNTING, EXECUTIVE DIRECTOR, NATIONAL FREEDOM OF INFORMATION COALITION, COLUMBIA, MISSOURI

Mr. BUNTING. I am Ken Bunting, executive director of the National Freedom of Information Coalition. We are a nonpartisan network of State and regional groups that work to promote open government and accountability. I am here today, early in the annual recognition of Sunshine Week, to ask that the principles of transparent, accountable government not become collateral damage as you wrestle with policy issues about critical infrastructure information and matters related to cybersecurity.

We recognize that there are circumstances under which information and details about the Nation's critical infrastructure need to be shielded from public dissemination. We also recognize that one of the legitimate goals of the various cybersecurity bills before you is creating a private industry comfort level with important information sharing.

But wherever exceptions to public access related to these matters reside in statute, we feel that they should include narrow definitions, a balancing test of the public interest in disclosure, and a sunset review process. I commend the Chairman for inserting narrowing language into the National Defense Authorization Act last December. Unfortunately, none of the cybersecurity measures before us now have similar provisions.

Nine years ago, a retired electrician named Glen Milner tried to find out something about the potential dangers he and his neighbors faced living near naval installations in the Puget Sound region

of Washington State. Mr. Milner wanted to know which parts of the coastal peninsulas and islands might see the greatest devastation in the event of an accidental explosion at the Navy's Indian Island facility. As you know, the Navy refused to provide that information, but the Supreme Court, in a ruling handed down last March, discredited the Navy's expansive interpretation of FOIA's Exemption 2. That case has now been remanded, and Mr. Milner and his lawyers are still doing battle in the legal arena for records he first requested in 2003 and over which he filed suit in 2006.

Now, I saw inescapable parallels as I watched the excellent MSNBC documentary about Master Sergeant Ensminger and the effects of three decades of toxic contamination at the Camp Lejeune Marine base in North Carolina. As the documentary crew portrayed it, Master Sergeant Ensminger and those who worked with him eventually came to recognize the shameful coverup, although they had begun with the expectation that the Marine Corps would do the right thing of its own volition.

The moral of this powerful story and so many others is that informed citizens with information to hold Government accountable provide the best incentive for things being done right.

We certainly do not belittle the concerns the legislative proposals before you seek to address. But please be leery of a broad, ill-defined sweep in closing off information. We believe any new cybersecurity or critical infrastructure exemptions should contain, at a minimum, a tight definition of the information to be exempted; a sunset for the law and for the protection attached to the information; and a public interest balancing test that allows legitimately protected information to remain protected, but not information being withheld primarily to protect the Government from embarrassment.

Under several proposals that have been put forth in the past 8 months, a 1995 "Dateline NBC" report that showed thousands of the Nation's dams close to collapse might not have been possible. Nor likely would a local TV report by University of Missouri students that showed only 33 of that State's 1,200 dams had the Emergency Action Plans required by law. And after-the-fact reporting by my old newspaper and others in Washington State—following a massive pipeline explosion that killed three innocent youths—would have been severely limited, reporting, by the way, that culminated, perhaps with a causal connection, in new pipeline safety legislation and a seven-count criminal indictment against two pipeline companies.

Without balancing tests and sunset provisions, health and safety information imprudently hidden from public view might remain shrouded in secrecy forever.

Just last week, nearing the 1-year anniversary of the Fukushima nuclear accident in Japan, the NRC released a heavily redacted report that used the ridiculously non-descriptive term "Generic Issue" to describe seismic and flooding hazards surrounding 35 domestic nuclear facilities. Given new criteria for withholding, their refusal to provide intelligible information will only get worse.

Please do not accept that cybersecurity and appropriate protections for critical infrastructure information pose a Hobson's choice with the people's right to know.

Senators, thank you for your invitation and for your attention. I look forward to your questions.

[The prepared statement of Mr. Bunting appears as a submission for the record.]

Senator GRASSLEY. [Presiding.] Thank you, Mr. Bunting.

For the Chairman, I will introduce Paul Rosenzweig, a visiting fellow at the Heritage Foundation's Center for Legal and Judicial Studies and Douglas and Sarah Allison Center for Foreign Policy Studies. Mr. Rosenzweig is also former Deputy Assistant Secretary for Policy at the Department of Homeland Security and Acting Assistant Secretary for International Affairs. He is a senior editor of the "Journal of National Security Law & Policy" and adjunct professor, Homeland Security at the National Defense University. He is a cum laude graduate of the University of Chicago Law School. He also has a M.S. in chemical oceanography from Scripps Institution of Oceanography, University of California at San Diego, and his B.A. is from Haverford College.

Thank you, Paul, for coming. Proceed.

STATEMENT OF PAUL ROSENZWEIG, RED BRANCH CONSULTING, PLLC, PROFESSORIAL LECTURER IN LAW, GEORGE WASHINGTON UNIVERSITY, AND VISITING FELLOW, THE HERITAGE FOUNDATION, WASHINGTON, DC

Mr. ROSENZWEIG. Thank you very much, Senator Grassley. I was checking my records, and this is the sixth time in the last 10 years that I have been in front of this Committee. It is always a pleasure to return to testify here.

Perhaps equally germane to my testimony today, I both teach cybersecurity law and policy at George Washington University and as a private consultant often speak of these issues with private sector clients who are vitally interested in pending cyber legislation.

My testimony today is restricted to the cybersecurity issues in front of us. I have no general issue at all with the premise that FOIA is an important aspect of transparency and should be broadly construed to promote the transparency of Government activity. I think, however, that the cyber threat is demonstrably different and that the pending proposals to provide for FOIA exemptions in the context of enhanced information sharing are right on point and, in my judgment, actually essential.

The cyber threat is real and likely quite enduring, and virtually everyone who has examined the issue in the private sector has concluded that the cheapest, most cost-effective way to get a running start at addressing that threat is through enhanced information sharing of cyber threat and vulnerability information, both between and amongst the private sector themselves and from the private sector to the Government, with the Government then being enabled to further share that information with others, both in Government and beyond.

Information sharing about cyber threat and vulnerability information is a bit like vaccination in the public health context. When one community knows of a virus threat and learns of how to cure it, it is essential for that information to be widely communicated throughout our community and throughout the world. Cyber threat information is fundamentally a public good.

In this context, it seems to me that the application of FOIA to cyber threat and vulnerability information voluntarily shared by the private sector with the Government turns FOIA on its head. The purpose behind FOIA, as demonstrated quite clearly both in the *Milner* case and in Sergeant Ensminger's case, is the transparency of Government functions. Thus, the main ground of a FOIA request is to seek information from the Government about Government and its operations.

Here, in the cyber context, the FOIA exemption contemplated is in relation to a private sector information sharing that would not otherwise—sharing of information that would not otherwise come into the Government's possession in the first instance. If we are serious about the cyber threat and if we seek the voluntary sharing of information in order to foster the creation of a clear and manifest public good, then the voluntary agreement of private sector actors to provide that information will, in the first instance, be contingent upon the Government's agreement not to subject them to adverse consequences.

Private sector actors, rightly, would see the absence of a FOIA exemption as a form of Government hypocrisy. We need the information, you will say, badly enough that we are asking you to provide it for the common good, but not so badly that we are willing to prevent that information from being shared with other private sector actors who, as your competitors or opponents in litigation, might wish you ill.

In my judgment, in the absence of a FOIA exemption, you will not get the private sector information sharing that is deemed essential, and it is not really just my judgment. The information-sharing provisions with accompanying FOIA exemptions are part of the Lieberman-Collins bill that has been introduced in this body, the McCain bill that has been introduced in this body, the bipartisan Rogers-Ruppersberger bill on the other side of the Hill, the bipartisan Lungren bill on the other side of the Hill, and I think most significantly is an integral part of the Obama administration's own legislative submission that they made to you in May of this past year.

Finally, I would close by saying that there is a real danger in subjecting cybersecurity threat and vulnerability information to the FOIA. Allowing public disclosure of such information would be identifying publicly which cyber threats are known risks, in effect drawing a road map of what threats are not known. That would have the substantive effect of drawing a target around the higher vulnerabilities, something that I think nobody would want to foster. Complete transparency, in my judgment in this instance, would defeat the very purpose of the disclosures that we are seeking voluntarily from the private sector and might even make us less secure.

Thank you very much.

[The prepared statement of Mr. Rosenzweig appears as a submission for the record.]

Chairman LEAHY. [Presiding.] Thank you very much.

Let me start with Sergeant Ensminger. First off, I, like all of us, thank you for your service to the country, but also as a parent and as a grandparent, I offer you my sympathy for what you went

through with Janey. I think what you tell us is that the transparency that we are supposed to have in FOIA is a promise to everybody in this country because it impacts the lives of Americans all across the Nation.

The public interest balancing test that Congress recently enacted in the National Defense Authorization Act, will that help you and others learn more about the well water contamination at Camp Lejeune?

Sergeant ENSMINGER. Yes, sir, but only if it is applied. In this instance, the National Defense Authorization Act was signed by the President at the end of December, and the United States Marine Corps sent a letter off on the 5th of January to another Government agency, which is part of the CDC, and that other Government agency did not question it. They just, for lack of a better term, rolled over into a fetal position and said, "Kick me again," and redacted—did everything in their bidding.

Chairman LEAHY. It is important that you make that point because, as I said, I intend to continue to follow up on this. Whether it is Senator Grassley or myself, Senator Cornyn or anybody else, we can pass all the legislation in the world with the right intentions. If it is not followed, then you are hurt, but so is everybody else. Is that correct?

Sergeant ENSMINGER. Yes, sir. And the information that they are trying to hold back from is the location of water supply wells, water towers, the water treatment plants aboard the base. I mean, for lack—I asked one of the Senate Committees—not a Committee but staffs the other day, they held a meeting with the Office of the Secretary of Defense and some of the representatives from the Marine Corps and the Department of the Navy concerning these redactions, and I jokingly asked them, before they went into the meeting, to please ask them if they perfected their Klingon-type cloaking device to cloak these 100-and-some-foot tall towers.

Chairman LEAHY. You see them when you drive by on the road.

Sergeant ENSMINGER. Yes, sir, and they are painted red and white checkered. I mean, what are they——

Chairman LEAHY. It is not a new form of camouflage.

Sergeant ENSMINGER. No, sir. And the water supply wells, many of them are out—not even within the gates of the base. They are along public highways, and the only physical security they have around them is a chain-link fence and a locked door to the pumphouse. Now, any terrorist that wanted access to those without physical security, they do not need to protect the information, the infrastructure information. They need more physical security, if they really, truly want to protect their people.

Chairman LEAHY. Well, when I am here in Washington, because of the house I have got in this area, I drive by a place with a big sign, "CIA." Well, that is fine. Everybody knows where it is. But it is protected.

Professor Bunting, you have experienced the FOIA process from the perspective of an academic, but also as a journalist. Do you have an idea how we could protect on the one hand the public's right to know while also protecting the Nation's cybersecurity? Mr. Rosenzweig talked about that before. Go ahead, sir.

Mr. BUNTING. Mr. Chairman, first of all, Professor Rosenzweig is the only cybersecurity expert at this panel. I do not pretend to be one. But with regard to FOIA, I think the worst thing would be a sweeping definition that was too broad, too loosely defined, where the words could be made to be whatever they wanted it to be, that gave too much unchecked power to the Government.

The reason we also ask that there be a review process, a sunset review process, in any new exemptions is exactly what Master Sergeant Ensminger just told you. It was only a couple of months ago that you put language in the NDAA to try and write a narrow definition and also a public interest balancing test. But, you know, is it going to be enforced? Time will tell.

Given any leeway, agencies will find a way to make it say what they want it to say, and so the key thing in protecting the public interest to know and not just tossing it out the window as you address these very real issues is to write a definition that is narrow enough, to make sure that the public interest is considered, and that you review it periodically going forward.

Chairman LEAHY. Thank you.

A vote has started. I will yield first to Senator Grassley and then Senator Whitehouse.

Senator GRASSLEY. Has it started? The light is not on up there yet.

Chairman LEAHY. Somebody will check.

Senator GRASSLEY. I will hurry along here then so that Senator Whitehouse can ask questions.

Chairman LEAHY. It started.

Senator GRASSLEY. OK.

Mr. Rosenzweig, I have a two-part question. First, when a business shares cyber threat information with the Government, what type of information are we talking about, a general description on your part? And, second, describe for us the type of damage that you believe would be done to the business sharing information and to our country if that cyber threat information was made public?

Mr. ROSENZWEIG. Well, thank you for the question. I will be brief in the interest of time, though obviously the answer to your first question is quite complex. But you can, broadly speaking, divide cyber threat information that would be shared into two bundles. One piece would be the actual malicious code and information, the IP protocols and ports that are being used, the websites, something that is quite specific to the threat itself. I can see no reason why we would ever want that information to be subject to FOIA because we would never want to broadcast more widely than is already shared that kind of threat information.

The other bundle of information is the data stream in which the threat resides, and that can be anything. It can be an e-mail attachment that is masquerading as an Excel spreadsheet. It can be the header information. It can be virtually any sort of content data. But that content data is really generally independent of the malicious code itself. It helps us identify the target that it is coming in Excel spreadsheets, but the content of that Excel spreadsheet, which could be a human resources spreadsheet or the company's salary data—it could be anything. In other words, malicious code can hide literally anywhere. So those are the two bundles.

The damage in the disclosure to the business obviously comes in the content information on the second side, which is, if they think that that content information is going to be subject to onward disclosure through FOIA, they are not going to provide it because that is usually CBI, confidential business information, proprietary information of some form. So what they are looking for is some assurance that the information they provide, which cannot be disassociated from a malicious code, will, in fact, be protected.

Senator GRASSLEY. In regard to that first part, you said if you could have a longer explanation. Maybe you could submit something in writing that would be more thorough than what you had time to give.

Mr. ROSENZWEIG. Sure.

[The information appears as a submission for the record.]

Senator GRASSLEY. My second question, and probably the last one——

Senator WHITEHOUSE. Senator Grassley, would you mind if I climbed onto that request so I get an answer as well? I am very interested in that same response.

Senator GRASSLEY. Of course, yes. So that will come from the two of us.

Mr. ROSENZWEIG. My pleasure.

Senator GRASSLEY. A two-part question. First, do you believe that the actually cyber threat information shared by a private company with the Federal Government provides no insights into how the Government operates as a Government? And, second, why should an open-government group ever need to have a copy of actual malicious code or virus given to the Federal Government by a private company?

Mr. ROSENZWEIG. As to the first of those, I can see no interest in an insight-into-government operation in having access to the underlying information from the private sector. I can see interest in learning how the Government treats what it does and whether or not we are responding well. But on the information itself, no. And as for the malicious code, I would say assuredly not. There is, in fact, a market—a black market, of course—in the sale of malicious code exploits because they are not generally widely known or used. When one is discovered, it is precious to the bad actor. It would be, to my mind, contrary to all sense of good public policy to make that more generally widely available so that it could be more readily exploited by a larger number of people.

Senator GRASSLEY. For you I have got two more questions, but I will yield back my time so Senator Whitehouse can ask questions and still get over to vote.

Chairman LEAHY. Senator Whitehouse.

Senator WHITEHOUSE. Thank you. I just wanted to follow up on Senator Grassley's line of questioning. The sort of information that would be provided from the private company in an information-sharing regime, would that ordinarily—if it had not been provided to the Government, would it ordinarily be amenable to any kind of FOIA access?

Mr. ROSENZWEIG. Not to my knowledge. FOIA does not run to the private sector, so if the wastewater treatment facility in Providence, Rhode Island, is under some sort of threat—unless it is a

publicly operated one. I do not actually know about Providence. But if it is a private sector one, it is not generally subject to FOIA, unless there is some State law that might apply that, again, I am not familiar with all 50 State laws, but generally no.

Senator WHITEHOUSE. So nothing that would otherwise be available to the public is taken from the public if information sharing is protected from FOIA.

Mr. ROSENZWEIG. That would be my understanding. We use the same model of protecting that type of critical infrastructure information that would not otherwise be available because it is voluntarily shared. In the PCII, the Protected Critical Infrastructure Information, that is shared under the Homeland Security Act, under the Chemical Facilities Antiterrorism Standards, sensitive security information about aviation, we use that model for private sector voluntary information quite frequently, and in general, the rule is it would not otherwise be available so we are not taking away something.

Senator WHITEHOUSE. Master Sergeant Ensminger raises the very good point that bureaucracies have not been unknown to use a variety of techniques to try to dodge disclosure—overclassification or unnecessary classification being one. Do you see a way in which legitimately available information could be shielded from public disclosure by some strategic use of the information-sharing regime? Somebody decides—I mean, I suppose the scenario would be an entity or organization that would otherwise have to make a disclosure of some kind, just sends the stuff in as information sharing even if it is not really legitimate to a cybersecurity complaint, and then says, Aha, you see, now I do not have to disclose it because I submitted it as the information sharing. Because of the nature of the beast, that strikes me as a phenomenon that we could probably guard against pretty successfully because it is not the natural purpose of the information-sharing effort. But what are your thoughts on that point of strategic abuse of the information sharing to quell public disclosure?

Mr. ROSENZWEIG. Your point is well taken, that is, that one could imagine a systematic effort by somebody to hide their own private sector malfeasance. That is going to be very unlikely and rare in the cybersecurity realm. There is not a lot of incentive that I see for trying to maintain vulnerabilities. The natural incentive is going to be for people who are aware of their own vulnerabilities to fix them because they suffer—the private sector suffers their own consequences for failing to fix that.

It strikes me that at this juncture, given the imminence of the cyber threat as we understand it, the value judgment that you need to make is whether or not that small likelihood means that you want to develop an exemption that would otherwise probably retard a lot of the sharing that is the plus value, or if you can come up with—my main answer to you, I think there is probably a mechanism for some sort of substituted transparency, which is not the full transparency of FOIA to the press and the public in this context, but institutions like the President's Civil Liberties and Oversight Board that you have already created or IGs or——

Senator WHITEHOUSE. Certainly you would want some form of ombudsman or IG to report on whether this was being abused in any way, wouldn't you?

Mr. ROSENZWEIG. I would certainly see room for something like that as a constructive proposal. I have not really thought it through that much.

Senator WHITEHOUSE. All right. I am about to be late to vote, so I am going to disappear.

Thank you, Chairman.

Chairman LEAHY. Thank you all very much. I will keep the record open for a couple days for follow-up questions. I did not mean to hurry you. You were asking perfect questions, and I apologize.

Thank you all very much.

Mr. BUNTING. Thank you, Mr. Chairman.

Mr. ROSENZWEIG. Thank you, Mr. Chairman.

[Whereupon, at 12:19 p.m., the Committee was adjourned.]

[Questions and answers and submissions for the record follow.]

QUESTIONS AND ANSWERS

QUESTIONS FOR THE RECORD FROM SENATOR CHARLES GRASSLEY

TO

MIRIAM NISBET

FOLLOWING THE SENATE JUDICIARY COMMITTEE HEARING:

"THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION AND THE PUBLIC'S RIGHT TO KNOW."

HELD ON MARCH 13, 2012

1. **The Office of Government Information Services (OGIS) was created to mediate disputes between the federal government and FOIA requestors.**

   (a) How many formal mediations has OGIS conducted in each fiscal year since it was created?

As explained below, OGIS has not conducted any formal mediations since it was created, however, during its first two fiscal years, OGIS opened 764 cases in response to requests for assistance — 391 in its first year and 373 in its second year, ending September 30, 2011. In June 2010, OGIS also began tracking phone and email "quick assists," and by the end of Fiscal Year (FY) 2011, the Office had helped nearly 500 callers and emailers.

The majority of OGIS cases—more than three-quarters in FY 2011—did not rise to the level of actual disputes. (OGIS defines true disputes as those cases in which the requester and the agency disagree about FOIA policies, procedures and compliance with FOIA or are at a communications impasse that goes beyond how to file a FOIA request, the status of a request and the like.) Of the 66 cases that OGIS identified as involving true disputes in FY 2011, two-thirds resulted in disputing parties agreeing to an outcome.

Congress used the term "mediation services" to describe OGIS's work. OGIS has interpreted "mediation services" as an umbrella term that includes the following: (1) Mediation, a voluntary and confidential process in which a neutral and independent third party, a mediator, assists disputing parties in reaching a mutually agreeable resolution; (2) Facilitation, one approach used by mediators to assist each party to communicate and to understand the other's position, interests and needs; and (3) Ombuds services, in which an ombudsman acts as a confidential and information resource, communications channel and complaint handler. OGIS's work providing mediation services is done in accordance with the Administrative Dispute Resolution Act (ADRA), 5 U.S.C. §§ 571-84, including its confidentiality provisions.

During OGIS's first two years, no cases resulted in formal mediation and the Office issued no advisory opinions. Several cases were ripe for mediation, but in those cases, both

parties could not agree on entering into mediation. (A well-established tenet of mediation is that it works best when both disputing parties agree to participate.) In one case, a Federal agency customer requested mediation, but the requester's attorney advised against it. In another case, despite nearly eight months of OGIS working to facilitate a resolution, the matter was still unresolved and the requester proceeded to litigation. In several cases, agencies reviewed and reaffirmed their final decisions and OGIS determined that the cases were not candidates for formal mediation.

(b) If there have been any formal mediations conducted by OGIS, who has conducted them? Are the mediators government employees or is OGIS hiring private mediators?

Although OGIS has not yet had to conduct a formal mediation, it does anticipate that it would use both government mediators and private mediators; the parties to a dispute must agree on the mediator and therefore the mediator could be either government or non-government. OGIS anticipates that it would bear the costs of hiring non-government mediators and the travel costs of government mediators, to the extent that the mediation could not be accomplished by teleconference or other technological means.

(c) If OGIS is paying private mediators, how much are they being paid?

OGIS has not yet had to hire a private mediator.

(d) How many OGIS employees are qualified to conduct mediations?

All six of OGIS's professionals are trained in mediation services. OGIS's three facilitators became certified in Federal workplace mediation in FY 2011 by Northern Virginia Mediation Service, an affiliate of George Mason University School of Conflict Analysis and Resolution. OGIS's Director, Deputy Director and staff attorney have completed mediation training offered by Pepperdine University's School of Law, Straus Institute for Dispute Resolution. Although OGIS has not, to date, handled any cases that have gone into formal mediation, it works regularly with government dispute resolution specialists and it has contacted several private professional mediators, all of whom are able to provide formal mediation should the need arise. In addition, OGIS continues to consider various mediation program models. OGIS's goal is to formally establish an effective and cost-efficient mediation program that can work with geographically dispersed parties as well as parties in and around the nation's capital.

(e) If OGIS employees are not qualified to conduct mediations, shouldn't a requirement for employment at OGIS be significant experience in conducting mediations?

OGIS's mission also includes review of agency FOIA policies, procedures and compliance. That portion of the mission is currently handled by every member of OGIS's professional staff. Although all six members are trained in mediation services, it is the view of

OGIS that, although helpful, significant experience in mediation services is not necessary for carrying out the review mission.

QUESTIONS FOR THE RECORD

Senator Amy Klobuchar

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

March 13, 2012

Questions for Miriam Nisbet

Do agencies vary significantly in terms of the process they use for analyzing FOIA requests with respect to critical infrastructure or generally? Would it be valuable for the statute to be more prescriptive with respect to the process for addressing these requests?

As you know, Federal agencies have distinct missions in fulfilling their statutory and regulatory responsibilities. Given the breadth of responsibilities of executive branch agencies, these missions involve varying levels of sensitivity and use of critical infrastructure information. For example, agencies with intelligence, law enforcement or foreign relations missions create and maintain sensitive records that are quite different than agencies that have oversight of financial institutions. It is in this context that Federal agencies analyze FOIA requests and consider agency-specific interests in determining whether information is appropriate for disclosure under FOIA. I look forward to working with you on whether a statutory change would, or would not, be helpful in this area, in light of the various missions and needs of agencies government-wide.

QUESTION FOR THE RECORD

TO

PAUL ROSENZWEIG

FOLLOWING THE SENATE JUDICIARY COMMITTEE HEARING:

"THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE INFORMATION AND THE PUBLIC'S RIGHT TO KNOW."

HELD ON MARCH 13, 2012

FROM SENATOR CHARLES GRASSLEY AND SENATOR SHELDON WHITEHOUSE:

Question: During the hearing, you were asked a two-part question by Senator Grassley. However, because of time constraints, you were only able to give abbreviated answers. Please provide complete answers to the following:

> First, describe the type of information involved when a business shares cyber threat information with the government.
>
> Second, describe the type of damage that you believe would be done to the business sharing the information and to our Country, if that cyber threat information was made public.

Answer: Information shared to reflect a cyber threat: As I said at the hearing cyber threat and vulnerability information generally falls into two bundles – the malicious code/threat itself and the data substrate in which the code arrived. A more formal analysis would expand on that shorthand summary in the following way:

The fundamental architecture of the Internet gives rise to the difficulty of distinction – it is a problem that is, in effect, built into the system. In a short hand way, all the 1s and 0s look the same.

Any successful cyber attack or intrusion requires "a vulnerability, access to that vulnerability, and a payload to be executed."[1] But in practice the first two parts of that equation (identifying a vulnerability and gaining access to it) are the same no matter what the payload that is to be delivered. Thus, for those attempting a defense, it is virtually impossible to distinguish *ex ante* between different types of intrusions because they all look the same on the front end: cyber espionage, where the intrusion is a payload that seeks to hide itself and exfiltrate classified data; cyber theft, where the object is stealing unclassified financial data; and a full-scale cyber attack, where the payload left behind may lie dormant for years before it is activated and causes grave cyber damage, cannot be readily distinguished as the software traffic is entering a system. The

[1] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," 4 *Journal of National Security Law & Policy*, 63 (2010).

difference arises only when the effects are felt. The closest kinetic world analogy would be something like never being able to tell whether the plane flying across your border was a friendly commercial aircraft, a spy plane, or a bomber.

This is not a readily soluble problem. All computer programs, including those used in cyber intrusions, are written in a programming language, often known as a source code. That source code is then compiled into the binary language understood by computers. To execute the program, or code, the computer reads the directions of the compiled binary language. This complex rendering from source code to executable instructions makes reading lines of computer code to discern their effect, in practice impossible. While different types of airplanes look functionally distinct from each other, computer code does not.

This circumstance changes only down the road, when an intrusion has been activated in one instance and the implementing code analyzed to reverse engineer the programming. Once that happens, a threat signature can be developed – and it is that threat signature that lies at the core of the pending information sharing proposals. Likewise, the analysis will often identify the particular gap, or vulnerability that is exploitable – a vulnerability that ought to be plugged once identified.

The information in question will relate, broadly speaking, either to specific threats from external actors (for example, knowledge from an insider that an intrusion is planned) or to specific vulnerabilities (for example, the identification of a security gap in a particular piece of software). In both situations, the evidence of the threat or vulnerability can come in one of two forms: either non-personalized information related to changes in types of activity on the network, or personalized information about the actions of a specific individual or group of individuals.

Network traffic information can relate to suspicious packets, including ports, protocols, and routing information; specific virus/other malware signatures; IP addresses; and the identification of particularly suspect domains or servers. Personally Identifiable Information (PII) includes more person-specific types of information such as identifying web sites accessed; times and locations of logins/account access; discrepancies in user names; or content of communications. It is typically related to a specific malfeasant activity (such as an attempted fraud, identify theft or the transfer of terrorist finances).

Once threats and vulnerabilities are known, we want them widely distributed. Thus, the first "bundle" of information constituting cyber threat and vulnerability information will be identified malicious source code and/or specific vulnerabilities within system that are capable of being exploited.

The other "bundle" of information will be the surrounding data within which the malicious code is secreted – in other words, the non-malicious code that represents the legitimate data stream being screened. Building on the description above, it is the non-malicious web sites accessed; the correct user names; or the legitimate IP addresses. It can also be the content within which the code arrives – an Excel spreadsheet for example, or perhaps a Word document (both have been used in recent years for the intrusion of a malicious Trojan horse program). It might be the email text with legitimate information that prefaces a malicious phising hot link.

This second bundle of information can be equally critical in identifying a vulnerability or threat methodology. Knowing the particular nature of an attack allows us to educate recipients on potential vectors of attack. But, critically, describing those vectors may not (indeed typically will not) require knowledge of the actual content – the nature of the attack is independent of the content data within which the attack resides.

Damage from publicizing threat and vulnerability information: Just as there is a market in producing cybersecurity there is also a market in producing cyber vulnerabilities. Knowledge of those vulnerabilities is a valuable commodity with commercial value. Should anyone doubt that there is such a private market consider the sale of zero-day exploits (that is, previously unknown vulnerabilities). Cyber hacker entrepreneurs expend great intellectual capital in discovering these exploits and marketing them on the black market. Truly unique and unusual zero-day exploits can sell for as much as $50,000. There is even a royalty provision in some sales where the discoverer gets a continuing payment for as long as the vulnerability remains unpatched.[2]

Given how difficult it is to discover vulnerabilities of this sort, it follows that the premature or unnecessary public disclosure of those vulnerabilities has the potential for doing grave damage to security interests. This is so because, in a resource-constrained world, even after a vulnerability is discovered it may take a period of time (sometimes quite substantial) before that vulnerability can be patched.

To cite a notable recent example, many of our legacy manufacturing control systems (known as SCADA systems) are vulnerable. The recent Stuxnet attack on Iran demonstrated that. But these SCADA systems are also quite old, deeply integrated into production processes and, unfortunately, difficult to patch. Yet replacing them is exceedingly expensive. The realistic prospect is that many of their vulnerabilities will remain in existence for a substantial period of time.

Fortunately, given the complexity of most SCADA systems it is highly unlikely that particular vulnerabilities will be readily discovered or widely known. Public disclosure of those vulnerabilities would have the perverse effect of disseminating information that, in any rational world, the system operator (and all of its customers) desperately hope to have remain confidential.

FROM SENATOR CHARLES GRASSLEY:

Question: Please provide any additional thoughts that you might have on the issues raised by the hearing, including but not limited to expanding on your testimony and/or responding to the testimony of the other witnesses.

Answer: Thank you very much for the opportunity to amplify on my answers. However, after reviewing the hearing transcript and the written testimony of the other witnesses I do not have any additional thoughts to add to the Committee's record.

---

[2] Charlie Miller, *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*, (Independent Security Evaluators 2007), http://weis2007.econinfosec.org/papers/29.pdf.

FROM SENATOR AMY KLOBUCHAR

Question: The Supreme Court decision in *Milner* limited the extent to which critical infrastructure information can be shielded by FOIA Exemption 2. Given that ruling, how can the current FOIA statutory scheme best be modified in order to protect critical government security information?

Answer: Since *Milner* there has been significant confusion within the Federal government. Despite the suggestion of the Supreme Court that other exemptions might be applicable, it has become clear that a great deal of critical security information that it is reasonable to withhold has become subject to disclosure. In practice this has led separate programs to seek so-called (b)(3) exemptions for specific types of information. In general, that sort of piece-meal approach ought to be disfavored and Congress should prefer a more uniform response. The most reasonable solution, in my judgment, would be for Congress to restore the *status quo ante* by legislatively enacting the old "high 2" exemption into law – perhaps limited by adopting a definition of critical infrastructure to which the exemption might apply. One model for an appropriate definition would be that used in the Homeland Security Act to define protected critical infrastructure information.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 12, 2012

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Melanie Pustay, Director of the Office of Information Policy, before the Committee on March 13, 2012, at a hearing entitled: "The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know."

Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Judith C. Appelbaum
Acting Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Minority Member

Written Questions to Director Melanie Pustay
Hearing On "The Freedom Of Information Act: Safeguarding Critical Infrastructure Information And The Public's Right To Know"

Chairman Leahy

DOJ FOIA Regulations

1. Last year, I worked with the Attorney General to address concerns that the Department of Justice's proposed new FOIA regulations would instruct federal agencies to mislead the public about the existence of government records that are subject to one of the exclusions under the Freedom of Information Act (FOIA). I understand that the Department is in the process of finalizing the regulations in a manner that will ensure more transparency and candor going forward.

a. When will the new FOIA regulations be finalized and made available to the public?

Response: The Department has completed its review of the comments received on its proposed new FOIA regulations, and proposed changes currently are under review.

b. Are federal agencies currently responding that "no responsive records exists" when they receive requests for records that are subject to a FOIA exclusion?

Response: As you know, Congress excluded certain records from the FOIA in 1986 to protect three narrow categories of criminal law enforcement and national security records when disclosure of even the existence of the records could compromise vital interests. The first category of excluded material addresses those situations where a requester seeks information relating to an ongoing criminal investigation, of which the target is unaware, and when even acknowledging the existence of responsive records would interfere with the enforcement proceedings. The agency may, during the time these circumstances apply, treat those records as not subject to the requirements of the FOIA. The second exclusion, which applies only to criminal law enforcement agencies, similarly protects against disclosures that would identify an informant, while the third exclusion, which applies only to FBI records, protects against disclosures of foreign intelligence or counterintelligence or international terrorism records, where the existence of the records is classified.

Because exclusions apply to circumstances where the existence of the requested records is itself the protected fact, they cannot be applied like exemptions, where the records are acknowledged, but withheld. Moreover, using a "Glomar" response for excluded records, i.e., where the agency neither confirms nor denies the existence of the requested records, would similarly not be effective or practical because there would be so many requests that would need to be Glomared. Agencies would need to Glomar every request that is received where an exclusion could potentially apply, which would include any request an individual makes on himself or herself, another individual, a company, or a private organization. Furthermore, Glomar responses must be openly linked to applicable FOIA exemptions, which again would be problematic in the three

specific contexts addressed by exclusions because citing the applicable exemption would reveal the protected interest covered by the exclusion. Because of these concerns, in those exceptional circumstances where a FOIA exclusion was invoked, agencies historically have responded to the request as if the excluded records did not exist. Such a response was based on the premise that when a requester makes a request pursuant to the FOIA, either implicit or explicit in the request is that he or she seeks records that are subject to the FOIA. This response has been uniform, across all administrations, ever since Congress excluded these records from the FOIA in 1986.

After further deliberation and review, the Department has decided there is a different way to implement the statutory exclusion provision that preserves the integrity of the sensitive law enforcement records at stake, while continuing to maintain the Department's commitment to being as transparent about that process as possible. As a result, the Department has withdrawn Section 16.6(f)(2) of its proposed FOIA regulations. The wording of response letters is now addressed instead through policy guidance issued by OIP on September 14, 2012, which instructs agencies on the appropriate language to use to notify requesters of the potential applicability of exclusions.

In yet another effort to bring greater transparency to the use of exclusions, the Department instituted a new reporting requirement on exclusions. In March 2012, agencies began to publicly report in their Chief FOIA Officer Reports the number of times that they invoked an exclusion during the prior fiscal year. This new reporting requirement not only promotes greater accountability, but also provides greater transparency on agencies' use of the statutory exclusions. As reported in agencies' 2012 Chief FOIA Officer Reports, in Fiscal Year 2011, only three agencies out of the ninety-nine subject to FOIA – the Department of Justice, the Department of Homeland Security, and the Environmental Protection Agency – reported invoking a statutory exclusion. These agencies collectively reported using an exclusion in response to 178 requests, which amounts to 0.03% of the 631,424 requests processed by the government in Fiscal Year 2011.

As you are aware, the Department also took several steps when drafting its proposed new FOIA regulations to bring its handling of exclusions in line with Attorney General Holder's commitment to open government. For example, Section 16.6(f)(1) of the Department's proposed new regulations requires components to obtain prior approval from OIP before invoking an exclusion, and Section 16.6(f)(3) requires that they maintain records of any uses of an exclusion and its approval. Finally, in order to promote greater public awareness of exclusions, Section 16.4(a) of the proposed regulations advises requesters that excluded records are not considered responsive to a FOIA request.

Moreover, in order to ensure that exclusions are properly invoked, the Department has for over twenty years encouraged agencies to consult with OIP in each instance when contemplating the use of an exclusion. Senior attorneys on my staff designated as exclusion experts work with these agencies to carefully determine whether the use of an exclusion is appropriate and absolutely necessary.

My Office is actively examining additional policies that would shed further light on agencies' handling of exclusions. We have recently issued government-wide guidance to agencies on this

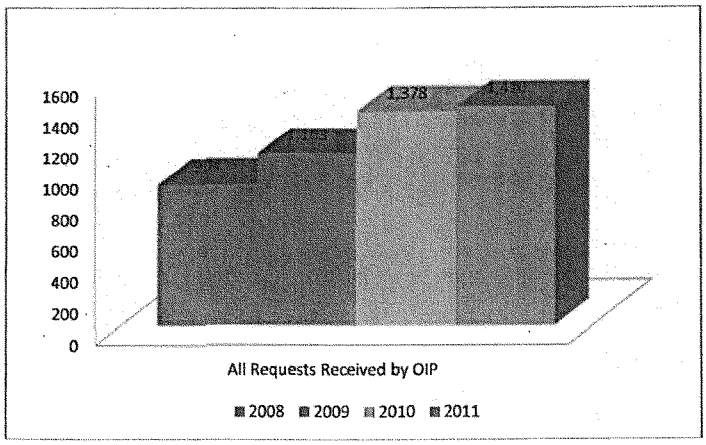
very important issue, and will be providing training that will assist agencies in properly using exclusions in the most transparent way possible.

Senator Cornyn

2. I am very concerned about the Freedom of Information Act (FOIA) request backlog in the Justice Department's three top leadership offices. According to the Department's own numbers, the offices of the Attorney General, Deputy Attorney General, and Associate Attorney General actually increased their backlogs over the past two fiscal years, FY10 and FY11. *See* Department of Justice Annual FOIA Report FY10, *available at* http://www.justice.gov/oip/annual_report/2010/sec12.pdf; **and Department of Justice Annual FOIA Report FY11, *available at*** http://www.justice.gov/oip/annual_report/2011/sec12.pdf. **The reported FY10 backlog was a 33 percent increase over the previous year. And the reported FY11 backlog was more than a 35 percent increase over FY10.**

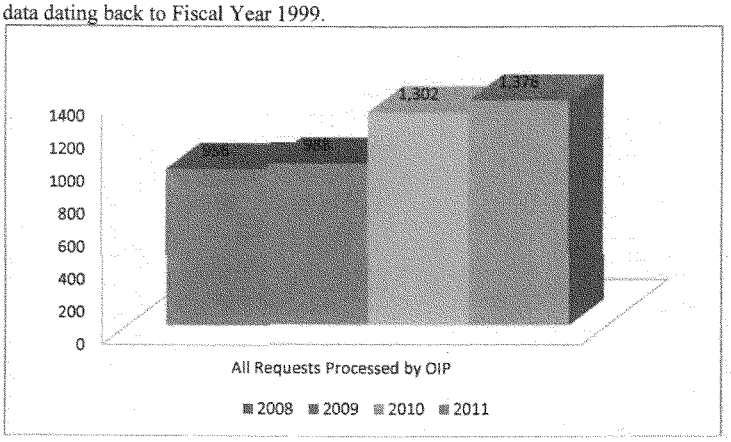
a. Please explain the reason(s) for these backlog increases.

Response: In Fiscal Year 2011, OIP's Initial Request Staff processed requests for a total of eight components. The increase of backlogged FOIA requests in the Offices of the Attorney General, Deputy Attorney General, and Associate Attorney General is largely attributed to the dramatic increase in incoming requests received by these offices, as well as the five other offices for which OIP processed records. In Fiscal Year 2008, the offices for which OIP processes records received 904 requests. In Fiscal Years 2009 and 2010, these offices experienced a 22% and 24.9% increase of incoming requests, respectively. This past fiscal year, the number of requests received by these offices reached a record high of 1,410, which is 506 (or 56%) more than was received in Fiscal Year 2008.

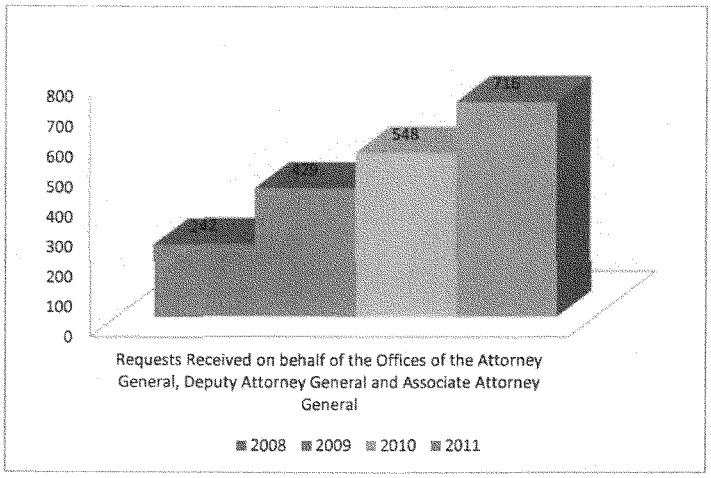


In an effort to match these dramatic increases of incoming requests, OIP has processed more requests each year since Fiscal Year 2009 when it processed 988 requests. In Fiscal Year 2010, OIP processed 1,302 requests, a 31.8% increase from the prior fiscal year. In Fiscal Year 2011, OIP processed 1,376 requests, which is the most requests processed by OIP based on available

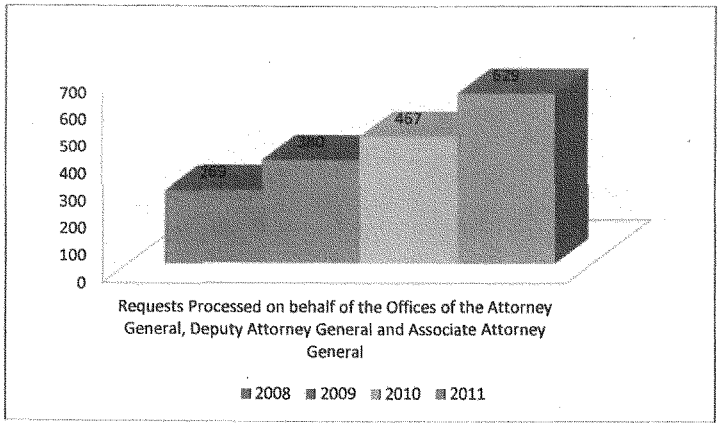
data dating back to Fiscal Year 1999.



The increased number of FOIA requests has had the most significant impact on the Offices of the Attorney General, Deputy Attorney General, and Associate Attorney General. Between Fiscal Years 2005 and 2009, these offices collectively received an average of 355 requests a year. This average increased by a significant 78%, rising to 632 requests between Fiscal Years 2010 and 2011. In fact, the number of requests received by these offices has increased every year since Fiscal Year 2009. In Fiscal Year 2009, these three offices collectively received 429 requests, which is a 77.3% increase from the prior fiscal year. The number of requests received by these offices increased by another 27.7% in Fiscal Year 2010. This past fiscal year, these offices collectively received 716 requests, a 30.7% increase from Fiscal Year 2010, and a significant 66.9% increase from the number of requests received in Fiscal Year 2009. In addition to the large increase of incoming requests, these offices have also received more complex requests that have demanded more time and resources to thoroughly process.



OIP has taken steps to increase its productivity to help meet the demand of the unprecedented numbers of requests from these offices and the increased complexity of those requests. In Fiscal Year 2009, OIP processed 380 requests for records maintained by these offices, which is a significant 41.3% increase from the prior fiscal year. OIP increased the number of requests processed for these offices by another 22.9% (467 requests processed) and 34.7% (629 requests processed) in Fiscal Years 2010 and 2011, respectively. Most significantly, between Fiscal Years 2008 and 2011, the number of requests processed for records in these offices increased by 133.8% from 269 requests in Fiscal Year 2008 to 629 in Fiscal Year 2011. These significant strides in increased processing reflect the dedication and commitment of OIP's staff.



b. How can your office serve as a leader of other Justice Department components, as well as a model for all other federal agencies, when it records significant backlog increases in back-to-back years?

Response: I am very proud of the example OIP and the Department of Justice has set in our leadership role with regard to the FOIA. Despite three straight years of receiving over 60,000 requests, this past fiscal year the Department increased the number of requests processed and reduced our backlog of pending requests by 26%. OIP achieved a parallel reduction in backlog by reducing the Department's backlog of administrative appeals by a full 41%. The Department also improved the average processing time for both simple and complex FOIA requests. Moreover, as explained above, in response to record numbers of incoming requests, OIP has achieved significant improvements in the number of requests processed, demonstrating its leadership in adjusting to unprecedented demand. OIP accomplished this while simultaneously continuing to fulfill its responsibility of encouraging agency compliance with the FOIA and ensuring that the Attorney General's FOIA Guidelines are fully implemented across the government. Since the issuance of the Attorney General's FOIA Guidelines, OIP has taken many steps to improve timeliness, increase responses, and reduce FOIA backlogs not only at OIP, but across all federal agencies.

OIP's efforts in this area have clearly been effective as the number of requests processed by OIP, the Department of Justice as a whole, and the entire government increased this past fiscal year. Serving as an example, OIP has increased the number of requests it processes every year since the Attorney General's Guidelines were issued. Additionally, since I became Director, OIP has specifically focused on reducing the age of the backlog at each of the eight offices for which we process records. To that end, I am proud to state that every year since Fiscal Year 2008, OIP has closed the ten oldest pending requests identified in the Department's Annual FOIA Report for each of those offices.

Moreover, embracing the President's call for greater use of technology in the FOIA process, OIP convened an inter-agency working group to explore ways in which technology can be better utilized to improve FOIA administration. OIP is currently pursuing a pilot to explore the feasibility of utilizing more sophisticated document management software to respond to FOIA requests. OIP is working to develop enhanced processing capabilities through use of technology with the goal of helping all agencies employ similar tools for the overall benefit of FOIA administration. Yet another example of OIP's leadership in FOIA administration is our work in issuing policy guidance. This past year, as part of our efforts to improve the FOIA process, and in direct response to concerns raised by open government groups, OIP issued guidance that provided new procedures for agencies to follow when handling document referrals and consultations. These new procedures are designed to maximize efficiency, promote accountability, and improve customer service.

3. The Associate Attorney General serves as the Justice Department's chief FOIA officer. According to the reports cited in Question 1 above, the Associate AG's backlog nearly doubled from FY10 to FY11.

a. Please explain the reason(s) for this backlog increase.

Response: While it is true that the number of backlogged FOIA requests at the Office of the Associate Attorney General went from 22 to 40 requests from Fiscal Year 2010 to Fiscal Year 2011, these raw numbers alone do not provide a full picture of the actual progress that the Office has made in processing FOIA requests. During Fiscal Year 2011, the Office of the Associate Attorney General experienced a 53% increase in incoming FOIA requests from the prior fiscal year, a significant portion of which were complex requests. In an effort to meet this demand, OIP processed substantially more requests on behalf of the Office of the Associate Attorney General, as well as the other seven offices for which we process records from Fiscal Year 2010 to Fiscal Year 2011.

b. What message do you think it sends to DOJ components and other federal agencies when the Justice Department's own chief FOIA officer nearly doubles his/her backlog in a single year?

Response: OIP and the Office of the Associate Attorney General stand by the example we have set for agency compliance with the FOIA and the implementation of the Attorney General's FOIA Guidelines. Here at the Department, despite three straight years of receiving over 60,000 requests, this past fiscal year we increased the number of requests processed and reduced our backlog of pending requests by 26%. OIP achieved a parallel reduction in backlog by reducing the Department's backlog of administrative appeals by a full 41%. In addition to making significant strides in reducing the backlog, the Department also improved the average processing time for both simple and complex FOIA requests. Both the Associate Attorney General and I have stressed the importance of agencies' efforts to reduce their backlogs in our FOIA leadership roles. However, we also understand that circumstances beyond an agency's control can sometimes make achieving this goal more difficult and that the full scope of an agency's accomplishments should be considered when assessing compliance with the Act. OIP has processed substantially more requests on behalf of not only the Office of the Associate Attorney General, but also the Offices of the Attorney General and Deputy Attorney General, and has closed the ten oldest pending requests in these offices as identified in the Department's Annual FOIA Report every year since Fiscal Year 2008.

Senator Grassley

4. An article in the November 2011 issue of the *Harvard Law Review* concluded that the practical effect of the Supreme Court's ruling in *Milner v. Department of the Navy* "will be to leave unprotected a great deal of information that could threaten the public safety if disclosed."[1] What is your reaction to that analysis? Do you agree with it or disagree with it? Please explain your answer in detail.

Response: The Department does have concerns about the impact of the Supreme Court's ruling in *Milner v. Department of the Navy*, 131 S. Ct. 1259 (2011) on the ability of agencies to adequately protect information that, if disclosed, could risk circumvention of the law. *Milner's* rejection of "High 2" overturned a three-decade-old approach to protecting these types of sensitive information. Although my Office has issued guidance (copy enclosed) on alternative FOIA exemptions that could potentially protect some information previously covered under "High 2," it is unlikely that the existing FOIA exemptions will suffice to protect, in all instances, every category of information whose release could cause harm. For example, the most likely exemptions that could protect the sensitive information left exposed by *Milner* are Exemptions 1, 3, and 7. As Justice Breyer pointed out in his dissent, reliance on Exemption 1 is not a practical solution as classification takes time and over-classification will undoubtedly hinder, among other things, information sharing between federal, state, and local agencies that is essential to preserving public safety. *See id.* at 1277 (Breyer, J., dissenting). In the wake of *Milner*, some agencies have sought statutory relief from mandatory disclosure under the FOIA for discrete categories of records they maintain. This piecemeal approach, however, of using separate withholding statutes that fall under Exemption 3 is also not an ideal solution as it does not sufficiently ensure protection for all agencies and all sensitive information. Similarly, not all sensitive information previously covered under "High 2" can easily satisfy the threshold requirement of Exemption 7, which is that the information must be "compiled for law enforcement purposes."

The Department believes that the preferred course of action for safeguarding information previously covered under "High 2" is to amend Exemption 2 so that its plain language addresses the need to protect against disclosures that would risk circumvention of the law. The precise contours of a proposed legislative amendment to Exemption 2 will of course need to take into account the important interests of preventing circumvention of the law and safeguarding national security as well as ensuring that exemptions are precisely crafted so as not to sweep too broadly. The Department is actively considering an appropriate solution that protects both these interests and is working with other Departments that have been impacted by the *Milner* decision. We also look forward to working with the Committee on this matter.

[1] **"Leading Cases," 125 HARV. L. REV. 341, 341-42 (2011).**

5. On March 30, 2011, the House Committee on Oversight and Government Reform released its 153-page report on its investigation of DHS's political vetting of FOIA requests.[2] The Committee reviewed thousands of pages of internal DHS e-mails and memoranda and conducted six transcribed witness interviews. It learned through the course of an eight-month investigation that political staff under Secretary Napolitano has exerted pressure on FOIA compliance officers, and undermined the federal government's accountability to the American people.
The report by Chairman's Issa's Committee reproduces and quotes email from political staff at DHS, including the Chief Privacy Officer. The report also quotes the transcripts of witness interviews. The statements made by the political staff at DHS are disturbing.

a. What is your response to each of the findings contained on pages 5-7 of the report?

b. What is your response to the disturbing statements made by DHS political staff, including the Chief Privacy Officer, who are quoted in the report? In particular, what is your response to political appointees in Secretary Napolitano's office referring to a career FOIA employee, who was attempting to organize a FOIA training session, as a "lunatic" and to attending the training session, for the "comic relief"?

Response to (a) and (b):

The Department understands that the Department of Homeland Security's Office of the Inspector General has completed a comprehensive investigation of this matter and has issued a report that provides six recommendations for improving the efficiency of DHS's FOIA administration. Any questions regarding the report or this matter are best directed to DHS.

The Department's position on efficiency in the FOIA process has been clear. Under the Attorney General's FOIA Guidelines, agencies are directed to ensure that they have an effective system in place for responding to FOIA requests. The Guidelines emphasize that "[a]pplication of the proper disclosure standard is only one part of ensuring transparency. Open government requires not just a presumption of disclosure but also an effective system for responding to FOIA requests." The Guidelines also stress that "[t]imely disclosure of information is an essential component of transparency." Accordingly, if an agency employs procedures that are inefficient or that cause unnecessary delays in responding to requests, those procedures would be contrary to the Attorney General's Guidelines. Furthermore, as the Attorney General's Guidelines expressly states, the FOIA is everyone's responsibility and not just that of the FOIA professionals within an agency. As such, all federal employees should be aware of their obligations under the FOIA and work to assist their agencies' efforts to comply with the Act.

---

[2] The report is entitled "A New Era of Openness? How and Why Political staff at DHS Interfered with the FOIA Process" and is available at http://oversight.house.gov/images/stories/Reports/DHS_REPORT_FINAL_FINAL_4_01_11.pdf.

6. Both Chairman Issa's report and a report prepared by the Inspector General of DHS find that political staff at DHS lack a fundamental understanding of FOIA. What, if anything, has the Department of Justice done to directly address this issue?

Response: As part of our responsibility to encourage agency-wide compliance with the FOIA and to ensure that the Attorney General's FOIA Guidelines are fully implemented, OIP provides training to thousands of federal employees each year, both at the courses offered by OIP and at agency-specific FOIA conferences. OIP also provides training at conferences sponsored by the American Society of Access Professionals and other organizations. OIP gives executive briefings to senior officials at agencies upon request and I routinely meet with the Chief FOIA Officers of the cabinet agencies to engage them on important issues concerning FOIA administration. These training courses cover all aspects of the FOIA, from procedural considerations, to the scope of the exemptions, to the requirements for assigning fee categories and assessing fee waiver requests, to litigation considerations. Some of the attendees at these various sessions are political appointees. Although there is no requirement that any group attend FOIA training, OIP does believe that it is important for all agency personnel to be aware of their obligations under the FOIA. The Attorney General's Guidelines make clear that the FOIA is everyone's responsibility and not just that of the FOIA professionals within an agency.

Since 2010, I have personally met with the Department of Homeland Security's Chief FOIA Officer twice to discuss their administration of the FOIA and my Office has conducted six separate training sessions exclusively for DHS staff covering various aspects of the FOIA, including President Obama's Memorandum on the FOIA and Attorney General Holder's FOIA Guidelines, an overview of the FOIA's procedural requirements and its nine exemptions, fees and fee waivers, the proper procedures for handling document referrals and consultations, and separate, more specialized training on Exemption 2 after the Supreme Court ruling in *Milner* and Exemptions 5, 6, and 7(C).

In addition to providing training, OIP engages in a wide variety of initiatives to both oversee and assist agencies with their FOIA compliance. First, OIP publishes the *Department of Justice Guide to the FOIA,* which is a legal treatise addressing all aspects of the law, including all of its procedural provisions. The Guide is publicly available on OIP's website and can be accessed at www.justice.gov/oip/foia_guide09.htm. In addition to the Guide, OIP's website also contains summaries of all the most up-to-date FOIA case law organized by the various issues that arise under the Act. *See* www.justice.gov/oip/court-decisions.html. Second, OIP issues guidance to agencies on the proper implementation of the statute and the Attorney General's Guidelines, which is also available on OIP's website. *See* www.justice.gov/oip/oip-guidance.html. Third, OIP provides daily legal counseling services to all agency personnel, who can call OIP on a dedicated phone line and speak to an attorney about any matter connected with the administration of the FOIA. Fourth, agencies are required to send out two reports each year to the Department of Justice. The Annual FOIA Report contains detailed statistics regarding the numbers and disposition of FOIA requests, and the time taken to respond. The Chief FOIA Officer Report describes narratively the steps taken to improve transparency at the agency, including the steps taken to ensure that the agency has an effective and efficient FOIA process. OIP, in turn, reviews these reports, engages in outreach to agencies as needed, and prepares a summary of both reports. OIP posts these reports on its website at a central access point. *See*

www.justice.gov/oip/reports.html. OIP also makes all the detailed statistics on agency FOIA compliance available to the public graphically on the Department's new government-wide comprehensive FOIA website, FOIA.gov. Through all of these initiatives OIP is both encouraging proper compliance with the FOIA and ensuring agency accountability.

Senator Klobuchar

7. The Supreme Court decision in *Milner* limited the extent to which critical infrastructure information can be shielded by FOIA Exemption 2. Given that ruling, how can the current FOIA statutory scheme best be modified in order to protect critical government security information?

Response: The Department is concerned about the vulnerability of sensitive material such as critical infrastructure information in the wake of the Supreme Court's decision in *Milner v. Department of the Navy*, 131 S. Ct. 1259 (2011). *Milner* overturned a three-decade-old approach to protecting these types of sensitive information under what was termed "High 2." The Supreme Court's rejection of "High 2" in *Milner* was based on the plain language of Exemption 2. In turn, the Department believes that the best course of action for protecting the sensitive information previously covered under "High 2" is to amend Exemption 2 so that its plain language addresses the need to protect against disclosures that would risk circumvention of the law.

Of course, the precise contours of a proposed legislative amendment to Exemption 2 will need to take into account the important interests of preventing circumvention of the law and safeguarding national security as well as ensuring that exemptions are precisely crafted so as not to sweep too broadly. Given that agencies and the public have had three decades of experience with a far more robust Exemption 2, one that provided for protection against risk of circumvention of the law, and in light of the fact that there is legislative history supporting such a reading, amending the exemption to reinstate that protection should be informed by that prior experience and history.

OIP Guidance:

Exemption 2 After the Supreme Court's Ruling in *Milner v. Department of the Navy*

On March 7, 2011, the Supreme Court issued an opinion pertaining to Exemption 2 of the Freedom of Information Act, 5 U.S.C. § 552 (b)(2) (2006 & Supp. III 2009), that overturned thirty years of established FOIA precedents and significantly narrowed the scope of that exemption. *See Milner v. Dep't of the Navy*, 131 S. Ct. 1259 (2011). This guidance will discuss the newly defined contours of Exemption 2 in the wake of *Milner* and will address possible alternatives that agencies can consider to protect sensitive information that is no longer covered by Exemption 2.

The Supreme Court's Decision

At issue in *Milner* were maps and data detailing "'minimum separation distances' for explosives" which aid the Department of the Navy in designing and constructing storage facilities to hold weapons, ammunition, and other explosives stored at the Naval Magazine Indian Island in Puget Sound, Washington. *Id.* at 1263. A resident of Puget Sound had requested the maps and data, and the Department of the Navy withheld them under Exemption 2, "stating that disclosure would threaten the security of the base and surrounding community." *Id.* at 1264. The requester challenged the decision. The District Court for the Western District of Washington and the Court of Appeals for the Ninth Circuit both upheld the Navy's decision to invoke what was commonly called "High 2." *See id.* Specifically, the Ninth Circuit held that disclosure of the data and maps "'would risk circumvention of the law' by 'point[ing] out the best targets for those bent on wreaking havoc' — for example, '[a] terrorist who wished to hit the most damaging target.'" *Id.* (quoting Ninth Circuit opinion, 575 F.3d 959, 971 (9th Cir. 2009)).

The Supreme Court granted certiorari, citing "the Circuit split respecting Exemption 2's meaning," and reversed. *Id.* In a ruling that is limited to the scope of Exemption 2, the Supreme Court then held that "Exemption 2, consistent with the plain meaning of the term 'personnel rules and practices,' encompasses only records relating to issues of employee relations and human resources." *Id.* at 1271. Utilizing that newly developed interpretation of the exemption, the Court found that "[t]he explosives maps and data requested here do not qualify for withholding under that exemption." *Id.* The case was then remanded back

to the Ninth Circuit for consideration of the applicability of Exemption 7(F), 5 U.S.C. § 552 (b)(7)(F), to the data and maps. The Navy had asserted Exemption 7(F) as an alternative ground for protection of the material and that claim now remains open for the Ninth Circuit to address. *See id.*

The Supreme Court's Focus on the Text of Exemption 2

In reaching its decision, the Court began by stating that its "consideration of Exemption 2's scope starts with its text." *Id.* at 1264. The Court noted that although other court decisions had analyzed the meaning of the exemption, "comparatively little attention has focused on the provision's 12 simple words: 'related solely to the internal personnel rules and practices of an agency.'" *Id.* Of those words, the Court found, "[t]he key word" and "the one that most clearly marks the provision's boundaries" is the word "personnel." *Id.* That word, in common usage, "means 'the selection, placement, and training of employees and ... the formulation of policies, procedures, and relations with [or involving] employees or their representatives.'" *Id.*

The Court found that using this commonly understood definition of the term "personnel," the phrase "personnel rules and practices" in Exemption 2 should be understood to mean "rules and practices dealing with employee relations or human resources." *Id.* at 1265. Indeed, the Court held, all the rules and practices encompassed within Exemption 2 "share a critical feature: They concern the conditions of employment in federal agencies — such matters as hiring and firing, work rules and discipline, compensation and benefits." *Id.* The Court went on to note that other courts "have had little difficulty identifying the records that qualify for withholding under this reading: They are what now commonly fall within the Low 2 exemption." *Id.* The Court concluded by declaring that its "construction of the statutory language simply makes clear that Low 2 is all of 2 (and that High 2 is not 2 at all ...)." *Id.*

***Exemption 2 Before* Milner *— High 2" and "Low 2" Under* Crooker**

Prior to *Milner*, the leading interpretation of the meaning of Exemption 2 was that provided by the Court of Appeals for the District of Columbia Circuit in *Crooker v. ATF*, 670 F.2d 1051 (1981). It is from that decision that the concept of "Low 2" and "High 2" were first established. Under the interpretation of Exemption 2 given by the D.C. Circuit in *Crooker*, the statutory language was read to imply a two-part test: to qualify for protection the records had to be first "predominantly internal," and second either of no genuine public interest, or trivial, which was referred to as "Low 2," or be matters of a more substantial nature if the disclosure would significantly risk circumvention of the law, which was referred to as "High 2." *See id.* at 1073-74; *see also Schiller v. NLRB*, 964 F.2d 1205, 1207 (D.C. Cir. 1992); *Founding Church of Scientology v. Smith*, 721 F.2d 828, 830 (D.C. Cir. 1983).

As the Supreme Court noted in *Milner*, the D.C. Circuit had fashioned this two-prong test for Exemption 2 based on language contained in an earlier Supreme Court decision in *Department of the Air Force v. Rose*, 425 U.S. 352, 362, 369 (1976). In *Rose*, the Supreme

Court had rejected the argument that case summaries of honor code and ethics proceedings held at the United States Air Force Academy were encompassed by Exemption 2. *Id.* at 367. As the *Milner* Court described its holding in *Rose*, the honor code case summaries did not fall within Exemption 2 "because they 'd[id] not concern only routine matters' of merely internal significance." *Milner*, 131 S.Ct at 1262. Still, the *Rose* decision contained a "possible caveat" to that narrow interpretation of Exemption 2, with the Court stating that the narrow interpretation applied "'at least where the situation is not one where disclosure may risk circumvention of agency regulation.'" *Id.* (quoting *Rose*, 425 U.S. at 369).

After this decision in *Rose*, the D.C. Circuit in *Crooker* took the caveat provided by the Supreme Court in *Rose* and fashioned "High 2" as a means of protecting internal matters where disclosure would risk circumvention of the law. *See* 670 F.2d at 1074. The D.C. Circuit reasoned that this interpretation of the Exemption "flowed from FOIA's 'overall design,' its legislative history, 'and even common sense,' because Congress could not have meant to 'enac[t] a statute whose provisions undermined . . . the effectiveness of law enforcement agencies.'" *Milner*, 131 S.Ct. at 1263 (quoting *Crooker*, 670 F.2d at 1074). Over the years, the Courts of Appeals for the Second, Seventh, and Ninth Circuits adopted the D.C. Circuit's two-prong approach to Exemption 2. *See id.*

The Supreme Court in *Milner* described the effects of the *Crooker* decision as having "spawned a new terminology; Courts applying the *Crooker* approach now refer to the 'Low 2' exemption when discussing matters concerning human resources and employee relations and to the 'High 2' exemption when assessing records whose disclosure would risk circumvention of the law." *Id.* Notably, though, this characterization of what was historically covered by "Low 2" both *omits* the requirement that there be no public interest in disclosure and *includes* the requirement that the information be connected with "human resources and employee relations." *See id.* In fact, though, many cases decided under what used to be known as "Low 2" required that the information be of no public interest, or trivial, and at the same time did not demand that it necessarily be related to human resources and employee relations. *See, e.g., Hale v. DOJ*, 973 F.2d 894, 902 (10th Cir. 1992) (withholding checklist form used by FBI agents to assist them in consensual monitoring as well as administrative markings and document notations because such records constitute trivial matters of no genuine public interest); *Schiller v. NLRB*, 964 F.2d 1205, 1208 (D.C. Cir. 1992) (affirming withholding under "Low 2" of internal agency time deadlines and procedures, recordkeeping instructions, directions for contacting agency officials for assistance, and guidelines on agency decisionmaking); *Antonelli v. BOP*, 569 F. Supp. 2d 61, 65 (D.D.C. 2008) (protecting investigatory case file numbers as internal information of no genuine public interest); *Wheeler v. DOJ*, 403 F. Supp. 2d 1, 13 (D.D.C. 2005) (withholding document routing information of no genuine interest to public); *Maydak v. DOJ*, 362 F. Supp. 2d 316, 324 (D.D.C. 2005) (upholding nondisclosure of purchase order accounting numbers that are used for internal purposes and bear no significant public interest).

The Supreme Court's Rejection of Crooker

In *Milner*, the government argued for the adoption of *Crooker's* two-pronged interpretation of Exemption 2. *See Milner*, 131 S. Ct. at 1266. The Supreme Court,

however, found that such an argument "suffers from a patent flaw: It is disconnected from Exemption 2's text." *Id.* at 1267. The "High 2" test, the Court found, "ignores the plain meaning of the adjective 'personnel,' . . . and adopts a circumvention requirement with no basis or referent in Exemption 2's language." *Id.*

The government argued that both the legislative history of Exemption 2 and Congress' subsequent action in amending the FOIA in 1986 supported the adoption of the *Crooker* formulation. The Court rejected both those arguments. First, with regard to the legislative history of the exemption, the Court noted that at the time of the enactment of the FOIA, the Senate and the House issued conflicting reports on the new FOIA law. *See id.* The House Report appeared to support the "High 2" construction of Exemption 2 while rejecting the concept of "Low 2." *See id.* The Senate Report, on the other hand, supported solely the "Low 2" interpretation of the exemption. *See id.* While the Court noted that it had previously weighed in on the interpretation of Exemption 2 in *Rose* and found the Senate Report to be "the more reliable of the two," the Court went on to expressly declare in *Milner* that "the more fundamental point is what we said before: Legislative history, for those who take it into account, is meant to clear up ambiguity, not create it. . . . When presented, on the one hand, with clear statutory language and, on the other, with dueling committee reports, *we must choose the language*." *See id.* (emphasis added). Thus, for the Supreme Court, the legislative history of Exemption 2 does not control its interpretation since the text of the exemption is clear.

Second, in *Milner* the Court rejected the government's argument that Congress' 1986 amendment of Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), to contain a "circumvention of the law" standard constituted its "ratification" of the *Crooker* test. *See id.* at 1267-68. In rejecting that contention, the Court stated that *Crooker's* "High 2" formulation was so broad that it "renders Exemption 7(E) superfluous and so deprives that amendment of any effect." *Id.* at 1268. As such, the Court found, "if Congress had agreed with *Crooker's* reading of Exemption 2, it would have had no reason to alter Exemption 7(E)." *Id.* Moreover, Congress' decision to amend Exemption 7(E) and not Exemption 2 "suggests that Congress approved the circumvention standard only as to law enforcement materials, and not as to the wider set of records High 2 covers." *Id.*

The Supreme Court's Rejection of a "Clean Slate" Approach to Exemption 2

The final argument advanced by the government in *Milner* was for adoption of a "clean slate" approach to Exemption 2, based on its text, that would encompass "'records concerning an agency's internal rules and practices for its personnel to follow in the discharge of their governmental functions.'" 131 S. Ct. at 1269. This argument too, was rejected by the Supreme Court as too sweeping and not sufficiently focused on the ordinary meaning of the phrase "personnel rule or practice." *Id.* The Court found that the use of the word "personnel" in terms such as "personnel file," "personnel department," and a "personnel rule or practice" signify "not that the file or department or practice/rule is *for* personnel, but rather that the file or department or practice/rule is *about* personnel — i.e., that it relates to employee relations or human resources." *Id.* Because the sweep of the proposed "clean slate" interpretation of the exemption would be so broad, and "would tend

to engulf other FOIA exemptions, rendering ineffective the limitations Congress placed on their application," the Court found that to adopt it would "violate[] the rule favoring narrow construction of FOIA exemptions" and this it declined to do. *Id.* at 1270.

The Supreme Court's Conclusion

In concluding its opinion the Supreme Court expressly stated that it "recognize[d] similar information." 131 S. Ct. at 1270. Significantly, it also acknowledged that its decision "upsets three decades of agency practice relying on *Crooker*, and therefore may force considerable adjustments." *Id.* at 1271. The Court pointed out though, that agencies have "other tools at hand to shield national security information and other sensitive materials," citing to possible application of Exemptions 1, 3, and 7 of the FOIA, 5 U.S.C. § 552 (b)(1), (3), (7). *See Milner*, 131 S. Ct. at 1271. Indeed, the *Milner* case was itself remanded for consideration of Exemption 7(F). Finally, the Court pointed out that if existing exemptions "do not cover records whose release would threaten the Nation's vital interests, the Government may of course seek relief from Congress." *Id.* It declared: "All we hold today is that Congress has not enacted the FOIA exemption the Government desires." *Id.*

Thus, in light of the Supreme Court's newly established interpretation of Exemption 2, it held that the explosive maps and data at issue in *Milner* did not qualify for Exemption 2 protection. *See id.* As the Court explained, the data and maps "concern the physical rules governing explosives, not the workplace rules governing sailors; they address the handling of dangerous materials, not the treatment of employees." *Id.* at 1266. As a result, Exemption 2 was not available to protect the material.

Justice Alito issued a concurring opinion supporting the majority's textual reading of Exemption 2. Justice Alito stated that he wrote separately to "underscore the alternative argument that the Navy raised below, which rested on Exemption 7(F)." *Id.* at 1271.

Justice Breyer issued a lengthy dissent from the opinion. He summed up his views this way: "Where the courts have already interpreted Exemption 2, where that interpretation has been consistently relied upon and followed for 30 years, where Congress has taken note of that interpretation in amending other parts of the statute, where that interpretation is reasonable, where it has proved practically helpful and achieved common-sense results, where it is consistent with the FOIA's overall statutory goals, where a new and different interpretation would require Congress to act just to preserve a decades-long status quo, I would let sleeping legal dogs lie." *Id.* at 1278.

The New Parameters of Exemption 2

The question now is how much of Exemption 2 remains in the wake of *Milner*. As a starting point, the Supreme Court has made clear that the Exemption must be read according to its clear statutory language. That language provides for exemption of matters "related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552(b)(2). Thus, the old formulations of "High 2" and "Low 2" — which were based on

legislative history and not on this statutory language — no longer control. There is now just plain "Exemption 2," which is defined according to its text.

A. New Three-Part Test

Based on that text, and as set forth by the Supreme Court's decision in *Milner*, there are three elements that must be satisfied in order for information to fit within Exemption 2.

1. The Information Must be Related to "Personnel" Rules and Practices

First and most importantly, as the Supreme Court emphasized, the "key word" in the exemption and the one word which "most clearly marks the provision's boundaries – is personnel." *Milner, 131 S. Ct.* at 1264. Thus, to qualify for protection under Exemption 2, agencies must ensure that the information at issue satisfies the requirement that it relate to an agency's *personnel* rules and practices. The Supreme Court gave several examples of what it viewed as constituting such personnel rules and practices. It described them as encompassing "'the selection, placement, and training of employees and . . . the formulations of policies, procedures, and relations with [or involving] employees or their representatives.'" *Id.* (*quoting* Webster's Third International Dictionary 1687 (1966)). It also described personnel rules and practices as the rules "dealing with employee relations or human resources," which "concern the conditions of employment in federal agencies — such matters as hiring and firing, work rules and discipline, compensation and benefits." *Id.* at 1265. All these examples illustrate the close connection information must have with employment in order to constitute a "personnel rule and practice."

Significantly, this requirement is cabined by the Court's rejection of the proposition that the term "personnel rules and practices" could be read to encompass those rules and practices that are written "for" personnel. *Id.* at 1269. The Court found that such an interpretation of Exemption 2 could be accomplished "only by stripping the word 'personnel' of any real meaning," since "agencies necessarily operate through personnel." *Id.* Given that many documents generated by an agency "aid employees in carrying out their responsibilities," the Court held that such a broad interpretation of Exemption 2 "would tend to engulf other FOIA exemptions." *Id.* at 1270. Accordingly, Exemption 2 does not reach those rules and practices of an agency that are not themselves related to "personnel." This requirement of Exemption 2, which the Supreme Court held is the key requirement for the exemption, significantly limits its scope. For the three decades preceding *Milner*, agencies focused on whether information was "predominantly internal" — a term significantly broader than "personnel rule or practice." Now, after *Milner*, agencies can only consider Exemption 2 for matters that relate to an agency's *personnel* rules or practices.

2. The Information Must Relate "Solely" to those Personnel Rules and Practices

In addition to this key requirement, the Supreme Court made clear that there are two additional requirements for invoking Exemption 2, *see id.* at *1265 n.4*, both of which are also directly taken from the text of the exemption. Although the Court gives very little

attention to these other requirements, addressing them only in a footnote, the Court states that they too must be satisfied in order to protect information under Exemption 2. *See id.* The first of these additional requirements is that the information at issue must "relate solely" to the agency's personnel rules and practices. *See id.* The Court defines this phrase by its "usual" meaning, which is "exclusively or only." *Id.*

3. The Information Must be "Internal"

The last requirement is that the information must be "internal," meaning that "the agency must typically keep the records to itself for its own use." *Id.* As the Court noted, these additional requirements would typically be met for human resource matters. *Id.* They also form distinct requirements for Exemption 2 that must be met before it is invoked by agencies. In interpreting these last two requirements, the prior decision of the Court in *Rose* provides guidelines that remain applicable today.

Impact of the Rose *Decision in Determining Whether Information "Relates Solely" to "Internal" Rules and Practices*

In declining to adopt a reading of Exemption 2 that was based on legislative history, the Supreme Court in *Milner* rejected the old "circumvention of the law" theory for protecting material under what used to be known as "High 2." In doing so, the Court in *Milner* was addressing the "caveat" to its earlier interpretation of Exemption 2 announced in *Rose,* which had alluded to the possibility of a circumvention standard. In *Rose* itself, there was no concern with any possible circumvention of regulations or standards and so that issue was not addressed by the Court in that case. *See* 425 U.S. at 365. *Milner* has now disposed of the circumvention caveat, but the core holding in *Rose* remains. That holding, in turn, impacts the scope of the last two requirements of Exemption 2, i.e., the requirements that the information must relate "solely" to "internal" personnel rules and practices of an agency.

In *Rose,* the Supreme Court denied Exemption 2 protection for case summaries of honor and ethics code hearings concerning cadets at the United States Air Force Academy. *See* 425 U.S. at 355. These summaries concerned the discipline of cadets and so would readily qualify under *Milner* as pertaining to "personnel." In *Rose,* Exemption 2 was found inapplicable to the honor code summaries due to the "genuine and significant public interest" in their disclosure. *Id.* at 369. The Supreme Court "agree[d]" with the conclusion of the Court of Appeals for the Second Circuit which had found that the summaries fell outside of Exemption 2 because they "'have a substantial potential for public interest outside the Government.'" *Id.* at 367. The Court went on to state that "the general thrust of the exemption is simply to relieve agencies of the burden of assembling and maintain for public inspection matter in which the public could not reasonably be expected have an interest." *Id.* at 369-70. It further explained that the honor code case summaries "plainly do not fit that description," and "are not matter with purely internal significance." *Id.* at 370. Moreover, the Court found, "[t]hey do not concern only routine matters" and "[t]heir disclosure entails no particular administrative burden." *Id.* As a result, the Court held that the summaries could not be protected under Exemption 2. *See id.*

In ruling that Exemption 2 did not apply to matters "subject to a genuine and significant public interest," the Court focused on the unique role of the military and the importance and significance of discipline within its ranks. *See id.* at 368-69. It also "agree[d]" with the Second Circuit's conclusion that even apart from the public interest generated by the government itself concerning the workings of the Academy's honor code, "there would be interest in the treatment of cadets, whose education is publicly financed and who furnish a good portion of the country's future military leadership." *Id.* at 369. The Court also "agree[d]" with the Second Circuit's conclusion that this public interest "differentiate(s) the summaries from matters of daily routine like working hours, which in the words of Exemption Two, do relate 'Solely to the internal personnel rules and practices of any agency.'" *Id.* at 369 (quoting Second Circuit).

In *Milner*, the Court summarized its holding in *Rose* by stating that in that case it had "concluded that the case summaries did not fall within the exemption because they 'di[d] not concern only routine matters' of 'merely internal significance.'" 131 S. Ct. at 1262. The Court also noted that in *Rose* it had "suggested" that the exemption "primarily targets material concerning employee relations or human resources; 'use of parking facilities or regulations of lunch hours, statements of policy as to sick leave, and the like.'" *Id.* at 1262 (quoting Senate Report).

Thus, in assessing whether information relates "solely" to the "internal" personnel rules and practices of an agency, it is necessary for agencies to assess whether there is a "genuine and significant public interest in disclosure." When there is a genuine and significant public interest in disclosure, the material falls outside of Exemption 2 as that interest would preclude it from satisfying the requirements of Exemption 2 that it relate "solely" to the "internal" personnel rules and practices of the agency.

So, while the Court in *Milner* included a broad list of examples of personnel-related items covered by Exemption 2, items such as "rules and practices dealing with employee relations or human resources," and "such matters as hiring and firing, work rules and discipline, compensation and benefits," 131 S. Ct. at 1271, there likely will some records falling within these categories where disclosure will be of "genuine and significant public interest." In those cases, the information would not be eligible for protection under Exemption 2 because it would fail the tests for sole internality.

In the end, the twelve words of Exemption 2 are all given meaning in determining its scope. The exemption protects matters "related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552 (b)(2). There is no doubt that the primary criterion for determining the exemption's scope is now the requirement that the information be related to "personnel." To the extent the material requested also *relates solely* to the *internal* personnel rules and practices of an agency — which means there is no genuine and significant public interest in its disclosure, the material is eligible for protection. Such routine matters, while eligible for protection, are, however, excellent candidates for discretionary release under the Attorney General's FOIA Guidelines.

Attorney General Holder's FOIA Guidelines

In analyzing records for possible Exemption 2 applicability, agencies should be mindful to consider, as they should for all exemptions, Attorney General Holder's FOIA Guidelines. Those Guidelines encourage agencies to make discretionary releases and to not withhold records absent a determination that disclosure would cause foreseeable harm. Exemption 2 has always held great potential for discretionary releases. *See* OIP Guidance: President Obama's FOIA Memorandum and Attorney General Holder's FOIA Guidelines: Creating a New Era of Open Government (advising agencies that "[i]nformation covered by "Low 2" is, by definition, trivial to begin with, thus there would be no reasonably foreseeable harm from release, and discretionary release should be the general rule" and further advising that "[b]efore applying High 2 to a record, agencies should ensure that they are not withholding based on "speculative or abstract fears").

The opportunities to make discretionary disclosures of material technically protected by the newly defined Exemption 2 remain as viable as ever. Thus, before invoking Exemption 2, agencies should ensure that they first make a determination whether disclosure of the information at issue would cause foreseeable harm. The Supreme Court emphasized in *Milner* that the harm sought to be prevented by Exemption 2 was "'simply to relieve agencies of the burden of assembling and maintaining [such information] for public inspection.'" 131 S.Ct. at 1262 (quoting *Rose*, 425 U.S. at 369). Certainly, there will be many examples of matters relating solely to internal personnel rules and practices where there is no foreseeable harm from release as there is no real burden involved in assembling and maintaining the information. Indeed, it is often more burdensome to withhold information than it is to release it. In the absence of harm, the information should be released as a matter of discretion in accordance with the Attorney General's FOIA Guidelines.

Possible Alternatives to Exemption 2

Recognizing that its new interpretation of Exemption 2 "may force considerable adjustments" to agency FOIA processing, the Supreme Court itself discussed the potential applicability of other exemptions to sensitive records, including Exemptions 1, 3, and 7. *See Milner*, 131 S. Ct. at 1270-71. Indeed, as mentioned above, with regard to the records at issue in *Milner*, the court noted that while Exemption 2 was not applicable, the government could still pursue on remand its argument that Exemption 7(F) applied to them. *Id.* at 1271. For other cases likewise in litigation, this significant change to the scope of Exemption 2 could constitute an "extraordinary" circumstance under 28 U.S.C. § 2106 (2006), which would permit the government to raise new exemption claims after initial briefing. *See Ryan v. Department of Justice*, 617 F.2d 781, 792 (D.C. Cir. 1980).

In *Milner*, the court conceded that there might be instances where the existing FOIA exemptions would not allow for the withholding of records whose release could clearly be

harmful. *Id.* While acknowledging this reality, the Court stated that the remedy for agencies is to "seek relief from Congress" rather than from the courts. *Id.* In the absence of such Congressional relief, for records that were formerly withheld under the old "High 2" standard, but which do not now fit within the newly defined parameters of Exemption 2, agencies should carefully consider the applicability of other FOIA exemptions to the material. A comprehensive discussion and legal analysis of all the FOIA's exemptions, their requirements, and court interpretations, is contained in the *United States Department of Justice Guide to the Freedom of Information Act (2009 ed.).* Agencies should consult this reference volume when considering the possible applicability of other exemptions to information formerly protected under Exemption 2.

Exemption 1

First, for disclosures that could risk harm to national security, Exemption 1 of the FOIA, 5 U.S.C. § 552(b)(1), is potentially available to protect records from public disclosure. Such protection is available for information that meets the criteria for classification set forth in Executive Order 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010). To classify information the agency must find that its unauthorized release "reasonably could be expected to result in damage to the national security." Exec. Order No. 13,526, § 1.1. The Executive Order specifies categories of information that can be considered for classification. *See id.* § 1.4. Those categories include matters such as military plans, weapons systems, or operations; foreign government information or foreign relations or activities; intelligence activities or sources or methods; scientific, technological, or economic matters relating to national security; programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, or infrastructures related to national security; or development, production, or use of weapons of mass destruction. *See id.* Once classified, the information must then be properly marked and safeguarded. *See id.* §§ 1.6, 4.1.

The Supreme Court in *Milner* specifically noted that despite its ruling on the scope of Exemption 2, "the Government has other tools at hand to shield national security information and other sensitive materials," through, "[m]ost notably, Exemption 1 of the FOIA." 131 S. Ct. at 1271. The Court further noted that the "government generally may classify material even after receiving a FOIA request" and so "an agency therefore may wait until that time to decide whether the dangers of disclosure outweigh the costs of classification." *Id.* Thus, Exemption 1 is an alternative exemption that agencies can consider for particularly sensitive records that meet the classification requirements of the Executive Order.

Exemption 3

Second, Exemption 3 is another potential means for withholding sensitive information that is no longer covered by Exemption 2. Exemption 3 provides for the withholding of records that are themselves protected from public release by another statute. *See* 5 U.S.C. § 552(b)(3). To qualify under Exemption 3, the other statute must either 1) be an absolute prohibition on disclosure or 2) provide specific criteria for withholding or refer to particular types of records that should be withheld. 5 U.S.C. §

552(b)(3)(A). For any withholding statute enacted after the date of enactment of the OPEN FOIA Act of 2009, Pub. L. No. 111-83, 121 Stat. 2184, the statute must specifically reference Exemption 3 of the FOIA in order to qualify as an Exemption 3 statute.

Agencies should first consider whether there is an existing Exemption 3 statute that affords protection to any information that no longer qualifies for protection under Exemption 2. In the absence of an existing Exemption 3 statute, agencies can consider seeking relief from Congress in the form of a new Exemption 3 statute. The Supreme Court itself recognized that Exemption 3 offers "Congress an established, streamlined method to authorize the withholding of specific records that FOIA would not otherwise protect." *Milner*, 131 S. Ct at 1271. Despite the difficulties inherent in passing new legislation, if an agency determines that certain categories of highly sensitive information will regularly be at issue in future FOIA requests, pursuing an Exemption 3 statute might be advisable.

Exemption 4

Third, Exemption 4 may provide a legal basis for withholding certain sensitive records, providing those records were obtained from outside the federal government. Exemption 4 provides for, *inter alia*, the withholding of "commercial or financial information obtained from a person [that is] privileged or confidential." 5 U.S.C. § 552(b)(4). The term "commercial or financial" has been broadly defined by courts as encompassing any records in which the submitter has a commercial interest. *See, e.g., Pub. Citizen Health Research Group*, 704 F.2d 1280, 1290 (D.C. Cir. 1983). A "person" for purposes of Exemption 4 is also very broadly interpreted, applying to corporations, banks, and state or foreign governments, among other entities. *See, e.g.*, Nadler v. FDIC, 92 F.3d 93, 95 (2d Cir. 1996). Finally, in determining whether information is "confidential," agencies must apply different tests depending on the manner in which the information is provided to the government. *See, e.g., Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992).

First, if the information was provided to the agency voluntarily, it is subject to protection under Exemption 4 if it would not be customarily released to the public by the submitter of the information. *See id.* Second, if submission of the information was required by the government, there are three ways in which it can protected: 1) if disclosure would impair the government's ability to obtain necessary information in the future; 2) if disclosure would be likely to cause substantial harm to the competitive position of the person from whom the information was obtained; and 3) if disclosure would harm other identifiable governmental interests, such as agency program effectiveness. *See id.; see also National Parks & Conservation Ass'n v. Morton*, 498 F.2d 765, 770 n.17 (D.C. Cir. 1974). After *Milner*, information supplied from outside the federal government that no longer can be protected under old "High 2" may be eligible for Exemption 4 protection under the tests for either a voluntary or a required submission.

For example, if a nonfederal entity provides an agency with the plans for a nuclear power plant or other critical infrastructure, agencies should consider whether Exemption 4 might apply. Such plans would likely be of commercial interest to the owners or operators

of the plants or infrastructure and since those nonfederal government entities are "persons" under Exemption 4, the threshold will be met. If such plans were provided voluntarily to the agency and are not customarily released by the submitter, they could qualify for protection under the *Critical Mass* test. Conversely, if the plans were provided to the agency as a required submission, and otherwise satisfy the threshold elements of Exemption 4, they can be considered for protection under the third test for required submissions — interference with program effectiveness. Agencies charged with regulating the safety of power plants could determine that their program's effectiveness would be diminished if records were disclosed that could facilitate security breaches at the facility.

Similarly, for information provided to an agency by a bank, such as agency credit card numbers or bank account numbers, such records could readily satisfy the threshold of Exemption 4. This information could also be considered for protection under the program effectiveness test because if an agency were required to release bank account numbers and credit card numbers to the public, the effectiveness of the agency's programs would be undermined, as for example, by the possible fraudulent use of the requested information by the public.

Exemption 6

Fourth, agencies can consider the applicability of Exemption 6, which protects "personnel and medical files and similar files" when disclosure of the information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). The Supreme Court has previously held, based on its review of the FOIA's legislative history, that the term "similar file" should be interpreted broadly to include all information that "applies to a particular individual." *United States Department of State v. Washington Post Co.*, 456 U.S. 595, 602 (1982). To determine whether disclosure would constitute a clearly unwarranted invasion of personal privacy, agencies must first identify a privacy interest that is at stake. Again, the Supreme Court has previously ruled on this point and, drawing on "the common law and the literal understanding of [the term] privacy," held that privacy "encompasses the individual's control of information concerning his or her person." *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 763 (1989). That privacy interest must be more than *de minimis*. *Multi-Ag Media LLC v. USDA*, 515 F.3d 1224, 1229 (D.C. Cir. 2008). Once a privacy interest is identified, it must be balanced against any public interest in disclosure. To qualify as a FOIA-recognized public interest in disclosure the information must "shed[] light on an agency's performance of its statutory duties." *Reporters Committee*, 489 U.S. at 773. In the absence of a qualifying FOIA public interest in disclosure, the privacy interest will prevail. It is possible that information that previously was withheld under Exemption 2 could qualify for protection under Exemption 6. For example, telephone numbers and passcodes assigned to participants of a conference call could be protected under this exemption as those participants have a privacy interest in ensuring that no uninvited person is listening in on the call and there is no public interest in disclosure of such numbers.

Exemption 7

Fifth, and finally, agencies should consider whether Exemption 7 is available to protect information that no longer qualifies under Exemption 2. In *Milner* itself, the Navy's assertion of Exemption 7(F) for the explosives data and maps at issue will now be reviewed by the lower courts. In Justice Alito's concurring opinion in *Milner*, he opined that the phrase "compiled for law enforcement purposes" should be construed to encompass not only traditional law enforcement in the sense of investigating and prosecuting bad actors for crimes that have already occurred, but also preventative law enforcement and security, meaning the prevention of future illegal acts. 131 S. Ct. at 1272. In his words, "[t]he ordinary understanding of law enforcement includes not just the investigation and prosecution of offenses that have already been committed, but also proactive steps designed to prevent criminal activity and to maintain security." *Id.*

Justice Alito provided specific examples of this type of law enforcement activity, such as steps taken by Secret Service agents to protect federal officials and efforts made by law enforcement officers to prevent a terrorist attack. *Id.*; *see, e.g., Moorefield v. U.S. Secret Service*, 611 F.2d 1021, 1024 (5th Cir. 1980) (finding that records compiled to assist the Secret Service in protecting the lives and safety of the President and his family qualify under Exemption 7).

Similarly, Justice Alito pointed out that records not originally compiled for a law enforcement purpose, "may fall within Exemption 7 if they are later assembled for law enforcement purposes." 131 S. Ct. at 1273. He gives as an example "federal building plans and related information — which may have been compiled originally for architectural planning or internal purposes — [and which] may fall within Exemption 7 if that information is later compiled and given to law enforcement officers for security purposes." *Id.* Additionally, Justice Alito opines that "[d]ocuments compiled for multiple purposes are not necessarily deprived of Exemption 7's protection," since the "text of Exemption 7 does not require that the information be compiled *solely* for law enforcement purposes." *Id.* Thus, he opines that "it may be enough that law enforcement purposes are a significant reason for the compilation." *Id.*

Agencies should use these guidelines in determining whether the information at issue qualifies under Exemption 7. To fall within the threshold of Exemption 7 the information must have been compiled, either originally or at some later date, for a law enforcement purpose, which includes crime prevention and security measures, even if that is only one of many purposes for the compilation. If this threshold is met, then the agency will next need to consider whether the requirements of the various subparts of Exemption 7 are satisfied.

Two of the subparts of Exemption 7, in particular, are likely to be applicable to information that no longer qualifies under Exemption 2. First, there is Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), which protects records or information compiled for law enforcement purposes when production of such records "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." This exemption has been found

to apply to techniques and procedures used in civil as well as criminal law enforcement investigations. *See, e.g., Nowak v. IRS*, No, 98-56656, 2000 WL 60067, at *1 ((9th Cir. Jan. 18, 2000); *Mosby v. U.S. Marshals Serv.*, No, 04-2083, 2005 WL 3273974, at *5 (D.D.C. Sept.1, 2005). It has also been applied in the context of preventative law enforcement. For example, some courts have allowed the protection of details pertaining to "watch list" programs. *See, e.g., Asian Law Caucus v. DHS*, No. 08-00842, 2008 WL 5047839, at *4 (N.D. Cal. Nov. 24, 2008); *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1035-36 (N.D. Cal. 2005) (protecting "selection criteria" for lists and handling and dissemination of lists). Other courts have allowed the withholding of techniques used by agents to protect federal employees. *See, e.g., Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 337 F. Supp. 2d 146, 181-82 (D.D.C. 2004) (approving withholding of "firearm specifications" and "radio frequencies" used by agents protecting Secretary of Commerce); *U.S. News & World Report v. Dep't of the Treasury*, No. 84-2303, 1986 U.S. Dist. LEXIS 27634, at *8 (D.D.C. Mar. 26, 1986) (protecting Secret Service's contract specifications for President's armored limousine). Moreover, prior to *Milner*, Exemption 2 and Exemption 7(E) were often used in conjunction. *See, e.g., Voinche v. FBI*, 940 F. Supp. 323, 329, 332 (D.D.C. 1996) (approving nondisclosure of information "relating to the security of the Supreme Court building and the security procedures for Supreme Court Justices" under both Exemptions 2 and 7(E)). For such information no longer falling within Exemption 2, Exemption 7(E) alone could provide protection.

Second, Exemption 7(F), 5 U.S.C. § 552(b)(7(F), which protects records compiled for law enforcement purposes when disclosure "could reasonably be expected to endanger the life or physical safety of any individual" is another option agencies may consider for records no longer falling within Exemption 2 when the harm that is foreseen is harm to the safety of individuals. It is Exemption 7(F) that will be considered by the lower courts for the explosives data and maps at issued in *Milner* itself. Moreover, as Justice Alito noted in his concurrence in *Milner*, "the Navy has a fair argument that the [explosives data and maps] fall[] within Exemption 7(F)," given that they are used "'for the purpose of identifying and addressing security issues,' and for the 'protection of people and property on the base, as well as in [the] nearby community, from the damage, loss, death, or injury that could occur from an accident or breach of security.'" *131 S. Ct. at 1273* (quoting Government's brief). As such, Justice Alito opined that, assuming Exemption 7's threshold was satisfied, the explosives data and maps "may fall comfortably within Exemption 7(F)." *Id.*

Agencies may at times be faced with requests for similar types of records where their concern is that disclosure could cause harm to individuals. If the record satisfies the threshold of Exemption 7, including compilation for a preventative law enforcement purpose, it can potentially be withheld pursuant to Exemption 7(F). *See, e.g., Living Rivers v. Bureau of Reclamation*, 272 F. Supp. 2d 1313, 1321 (D. Utah 2003) (protecting "inundation" maps that could reasonably be expected to place at risk the lives of individuals who lived downstream in areas that could be flooded by breach of dams; finding that such inundation maps were used by the Bureau of Reclamation to aid in its law enforcement mandate to maintain law and order and to protect people and property within reclaimed lands, and further finding that disclosure "could increase the risk of an attack on

the dams"). *But see ACLU v. DOD*, 543 F.3d 59, 63, (2d Cir. 2008) (rejecting applicability of Exemption 7(F) to certain detainee photographs based on argument that release "could endanger United States troops, other Coalition forces, and civilians in Iraq and Afghanistan," finding that the phrase "individual" as used in Exemption 7(F) "may be flexible, but is not vacuous," and does not apply to "members of a group so large that risks which are clearly speculative for any particular individuals become reasonably foreseeable for the group"), *vacated & remanded*, 130 S. Ct. 777 (2009) (vacating and remanding for further consideration in light of newly enacted statute affording protection to certain photographs).

While Exemptions 1, 3, 4, 6, and 7 all serve valuable roles in protecting sensitive information that was formerly withheld pursuant to Exemption 2, it seems inevitable that there will be some sensitive records that will not satisfy the standards of any of the Exemptions. Indeed, Justice Breyer recognized this conundrum in his dissent. In criticizing the majority's holding and its acknowledgement that "considerable adjustments" may need to be made, Justice Breyer posits the question "how are these adjustments to be made?" 131 S. Ct. at 1277. He asks what can be done "for information that is *not* compiled for law enforcement purposes." *Id.* He notes that "classification is at best a partial solution," that "takes time" and "is subject to its own rules." *Id.* Likewise, legislative action "takes time" and Congress "has much to do." *Id.* Justice Breyer, therefore, believed that "Congress' public information objectives" were appropriately left to the courts to turn "into workable agency practice[s] and [that courts should] adhere to such interpretations once they are settled." *Id.* His views, however, did not persuade the majority.

Conclusion

In *Milner*, the Supreme Court overturned decades of judicial interpretation of the scope of Exemption 2. The exemption is no longer divided into "High 2" and "Low 2." Rather, a strict textual reading of the exemption must be now be employed, with the key requirement being a focus on the word "personnel." Only those matters "related solely to the internal personnel rules and practices of the agency" are eligible for protection under the newly defined Exemption 2. Agencies should consider making discretionary releases of such information in accordance with the Attorney General's FOIA Guidelines whenever they determine that release would not cause foreseeable harm. For those instances where there is foreseeable harm, and yet due to the narrowed scope of Exemption 2, the information can no longer be protected under that exemption, agencies should consider whether other exemptions afford protection. In making those determinations, agencies are encouraged to call OIP's FOIA Counselor line to discuss the matter. The Supreme Court's decision in *Milner* represents a landmark case in the history of the FOIA, and this guidance should serve as a starting point for agencies to work through its many implications for their FOIA-processing efforts.

SUBMISSIONS FOR THE RECORD

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.

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

March 12, 2012

Senator Patrick J. Leahy, Chairman,
Committee on the Judiciary
437 Russell Senate Office Building
Washington, D.C. 20510

Senator Chuck Grassley, Ranking Member
Committee on the Judiciary
135 Hart Senate Office Building
Washington, D.C. 20510

Dear Chairman Leahy and Ranking Member Grassley,

Thank you for holding the hearing on "the Freedom of Information Act: Safeguarding Critical Infrastructure and the Public's Right to Know." In response to your request for a written statement, we provide the following comments on the importance of the Freedom of Information Act, specifically concerning cyber security.

The Electronic Privacy Information Center ("EPIC") is a non-partisan research organization, established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] Much of EPIC's work over the years has been in support of the Freedom of Information Act and open government. EPIC pursued many Freedom of Information Act matters and litigated numerous cases.[2] EPIC has commented extensively on the proposed changes to the Department of Justice Freedom of Information Act regulations.[3] EPIC publishes a leading Freedom of Information Act litigation manual.[4] And we help train the next generation of Freedom of Information Act advocates and practitioners.[5]

Next week, we will be arguing before the D.C. Circuit in support of a narrow interpretation of the so-called "Glomar" doctrine.[6] We believe that the National Security Agency has improperly withheld from the American public information that should properly be released under the Freedom of Information Act. As the Congress is now considering cybersecurity legislation, we are grateful that you have taken the opportunity of Sunshine week to draw attention to the need for open and accountable government.

---

[1] EPIC, About EPIC, http://www.epic.org/epic/about.html (last visited Mar. 12, 2012).
[2] EPIC, EPIC FOIA Cases, http://epic.org/foia/ (last visited Mar. 12, 2012).
[3] Comments of the Electronic Privacy Information Center to the Department of Justice on "Revision of Department of Justice Freedom of Information Act Regulations" (Oct. 18, 2011), *available at* http://epic.org/foia/EPIC-DOJ-FOIA-Comments-FINAL.pdf.
[4] Harry A. Hammitt, Ginger McCall, Marc Rotenberg, *et. al, Litigation Under the Federal Open Government Laws* 2010 (EPIC 2010).
[5] EPIC, Jobs / IPIOP, http://epic.org/epic/jobs.html (last visited Mar. 12, 2012).
[6] *EPIC v. NSA*, Civ. Action No. 11-5233 (D.C. Cir. Sept. 9, 2011).

I. The Freedom of Information Act is Vital to Ensuring an Accountable and Transparent Government

Since the enactment of the Freedom of Information Act, Presidents have acknowledged the importance of open government to democracy. In signing the Freedom of Information Act in 1966, President Johnson acknowledged, "this legislation springs from one of our most essential principles: a democracy works best when the people have all the information that the security of the nation will permit."[7] When President Gerald R. Ford signed the Government in the Sunshine Act of 1976, amending the Freedom of Information Act, he asserted, "the decision-making business of regulatory agencies can and should be open to the public."[8] President Ford also showed particular concern over the language of Exemption Three, an issue now before this Committee, declaring that it "may well be more inclusive than necessary."[9] And President Clinton recognized that "the Freedom of Information Act was the first law to establish an effective legal right of access to government information, underscoring the crucial need in a democracy for open access to government information by citizens."[10]

When President Obama took office in 2008, he committed his administration to the importance of transparency in government. On his first day in office, President Obama issued a memorandum about the importance of the Freedom of Information Act. He explained, "At that heart of that commitment [to transparency] is the idea that accountability is in the interest of the Government and the citizenry alike."[11]

To further these goals, President Obama called for new guidelines for implementing Freedom of Information Act.[12] The guidelines issued by Attorney General Holder establish a "presumption of openness" governing federal records.[13] The Attorney General strongly encouraged agencies to make discretionary disclosures of information to the fullest extent possible. The memorandum directs that each agency is fully accountable for its administration of the Freedom of Information Act and should be mindful of their obligation to work "in a spirit of cooperation."[14]

---

[7] Signing Statement by President Lyndon Johnson on the Passage of S. 1160 the Freedom of Information Act (July 4, 1966), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB194/Document%2031.pdf.
[8] Signing Statement by President Gerald Ford on the Passage of S. 5 the Sunshine Act (Sept. 13, 1976), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=6325#axzz1oqLMGQp2.
[9] *Id.*
[10] Signing Statement by President William Clinton on the Passage of H.R. 3802 the Electronic Freedom of Information Act Amendments of 1996 (Oct. 2, 1996), *available at* http://www.gwu.edu/~nsarchiv/nsa/foia/presidentstmt.pdf.
[11] Memorandum from President Barack Obama to the Heads of Executive Departments and Agencies on Transparency and Open Government (Jan. 21, 2008), *available at* http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.
[12] *Id.*
[13] Memorandum from Attorney General Eric Holder to Heads of Executive Departments and Agencies on Transparency and Open Government (Mar. 19, 2009), *available at* http://www.usdoj.gov/ag/foia-memo-march2009.pdf.
[14] *Id.*

The Freedom of Information Act has been responsible for uncovering numerous cases of government fraud and abuse since its inception. Through proper and efficient use of the Freedom of Information Act, EPIC has brought to the public's attention many such matters:

- **Intelligence Oversight Board Records Revealed that the FBI was not in Compliance with Attorney General Guidelines.** EPIC obtained internal reports of intelligence law violations that the Federal Bureau of Investigation sent to the Intelligence Oversight Board. The documents detail intelligence practices that do not comply with Attorney General Guidelines.[15]

- **United States State Department Discloses Report on Obama Passport Breach.** EPIC's Freedom of Information Act lawsuit against the State Department produced a report detailing security breaches of passport data for several presidential candidates. Previously secret sections state, "the Department was ineffective at detecting possible incidents of unauthorized access," and criticized the agency's failure to "provide adequate control or oversight."[16]

- **General Services Administration Records Revealed that Feds Exempted Social Media Companies from Privacy Requirements.** In response to EPIC's Freedom of Information Act request, the General Services Administration released several contracts between the federal government and web 2.0 companies. Some of the agreements permit companies to track users of government websites for advertising purposes.[17]

- **Federal Bureau of Investigation Records Reveal Restriction of Virginia Transparency and Privacy Laws for Fusion Center.** A document obtained by EPIC from the Virginia Department of State Police reveals that the State Police entered into a secret agreement with the Federal Bureau of Investigation to impose federal restrictions on rights granted by Virginia open government and privacy laws.[18]

These revelations, and many more, were only possible through the meaningful application of the Freedom of Information Act. We will discuss the significant cybersecurity Freedom of Information Act matters EPIC has pursued in more detail below.

---

[15] *Intelligence Oversight Board: FOIA Documents Detailing Legal Violations*, ELEC. PRIVACY INFO. CTR., http://epic.org/foia/iob/default.html (last visited Mar. 12, 2012).
[16] *EPIC Forces Disclosure of Report on Obama Passport Breach*, ELEC. PRIVACY INFO. CTR., http://epic.org/open_gov/foiagallery2011.html#passport (last visited Mar. 12, 2012).
[17] *Feds Exempt Social Media Companies from Privacy Requirements*, ELEC. PRIVACY INFO. CTR., http://epic.org/open_gov/foiagallery2010.html#social (last visited Mar. 12, 2012).
[18] *EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/virginia_fusion/ (last visited Mar. 12, 2012).

II. There is a Considerable Public Interest in the Transparency of Government Cybersecurity Operations

The efforts by the government to protect our nation's critical infrastructure affect every citizen in the United States, whether or not they actually use the Internet. Information that provides details on cybersecurity threats and the failure of important information systems and databases is invaluable to every member of the U.S. population, a fact recognized by both Democrats and Republicans in the introduction and support of federal data breach notification bills.[19] People have a right to know about government decisions that impact their safety and their security.

On May 29, 2009, President Barack Obama announced the Administration's plan to address the growing issue of digital information insecurity.[20] Discussing the plan in 2010, Cybersecurity Coordinator Howard Schmidt emphasized the importance of transparency:

> Transparency is particularly vital in areas, such as the [Comprehensive National Cybersecurity Initiative], where there have been legitimate questions about sensitive topics like the role of the intelligence community in cybersecurity. Transparency provides the American people with the ability to partner with government and participate meaningfully in the discussion about how we can use the extraordinary resources and expertise of the intelligence community with proper oversight for the protection of privacy and civil liberties.[21]

Transparency and accountability in cybersecurity operations will promote security and encourage companies to implement meaningful data practices that reduce the risk of cybersecurity incidents. Companies must understand that at risk are not only their own records, but also information concerning their clients, customers, and users. For this reason, any proposal to reduce the information available to the public currently available under the Freedom of Information Act concerning cybersecurity risks should be viewed with skepticism.

III. Congress Recently Adopted a Narrow Exemption Three Statute for Critical Infrastructure

Congress has already passed an adequate Exemption Three statute to protect sensitive critical infrastructure information from disclosure under the Freedom of

---

[19] *See, e.g.*, Data Accountability and Trust Act (DATA), H.R. 1707, 112th Cong. (2011) (introduced by Rep. Rush (D-IL)); Secure and Fortify Electronic Data Act (SAFE Data Act) H.R. 2577, 112th Cong., (2011) (introduced by Rep. Bono Mack (R-CA)).

[20] WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[21] Howard A. Schmidt, *Transparent Cybersecurity*, NAT'L SEC. COUNCIL (Mar. 2, 2010), http://www.whitehouse.gov/blog/2010/03/02/transparent-cybersecurity.

Information Act.[22] Precisely, the exemption in the 2012 National Defense Authorization Act allows agencies to withhold "Department of Defense critical infrastructure" only:

> upon a written determination that the disclosure of such information would reveal vulnerabilities in such infrastructure that, if exploited would reveal vulnerabilities in such infrastructure that, if exploited, could result in the disruption, degradation, or destruction of Department of Defense operations, property, or facilities.[23]

While we would have preferred no such exemption, this provision is narrowly constructed to achieve the desired result. The legislation recognizes both the interests of ensuring the protection of "truly sensitive government information" and "allowing public access to important information about potential health and safety threats."[24]

IV. Pending Cybersecurity FOIA Proposals Would Limit Government Transparency and Accountability

The current cybersecurity legislative proposals contain Freedom of Information Act exemptions that are over-broad and will limit both accountability and transparency in United States cybersecurity operations. Notably, while most of the cybersecurity bills currently under consideration attempt to block any public access to cyber threat information, the provisions encourage the increased transfer of information to and between the private sector and the federal and state governments without any accountability for the negligent or willful misuse of that information.[25]

A. The Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012

The SECURE IT Act seeks to amend the Freedom of Information Act in an unprecedented manner by adding a tenth exemption for "information shared with or

---

[22] The Homeland Security Act of 2002 also contains an Exemption Three provision for voluntarily shared critical infrastructure information. Specifically, the Act protects "critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency, study, recovery, reconstitution, or other informational purpose." 6 U.S.C. § 133(a)(1) (2011).

[23] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81.

[24] Press Release, Sen. Patrick Leahy, Balancing Security And Open Government In The Cyber Age (Mar. 6, 2012), *available at* http://www.leahy.senate.gov/press/press_releases/release/?id=4add311a-6a53-4d37-aff6-09172c984c9d.

[25] *See* Cybersecurity Act of 2012, S. 2105, 112th Cong. § 704(f) (2012), *available at* http://www.govtrack.us/congress/billtext.xpd?bill=s11262105 [hereinafter *Cybersecurity Act of 2012*] (creating liability only for knowing *and* willful violations of the Act); Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act of 2012, S. 2151, 112th Cong. § 102(g) (2012) [hereinafter *SECURE IT Act*] (no liability for "use, receipt, or disclosure of any cyber threat information.").

provided to a cybersecurity center."[26] The SECURE IT Act also contains a proposed Exemption Three provision that would specifically exempt all "cyber threat information" shared with the government from disclosure.[27] "Cyber threat information" is defined broadly, and could include a large amount of information unrelated to cybersecurity.[28] And without any precedent, this new provision would be mandatory, prohibiting agencies from disclosing information even would it could be made routinely available. Such language could easily produce absurd results if, for example, an agency prepares a document that it is intended to be publically available and to assist the public respond to cyber threats. According to this proposed amendment, the agency would be prohibited from providing to the public under the Freedom of Information Act a public document that would assist in countering cyber threats. It is hard to imagine a more ill conceived policy.

In a letter to Senator McCain, the bill's author, civil libertarian groups explain the damaging effect the SECURE IT Act would have on government transparency:

> As drafted, S.2151 cuts off all public access to information in cybersecurity centers before the public has a chance to understand the types of information that are covered by the bill. Much of the sensitive information likely to be shared in the cybersecurity centers is already protected from disclosure under the [Freedom of Information Act]; other information that may be shared could be critical for the public to ensure its safety. Unnecessarily wide-ranging exemptions of this type have the potential to harm public safety and national defense more than enhance those interests; the public is unable to assess whether the government is adequately combating cybersecurity threats and, therefore, unable to assess whether or how to participate in that process.

EPIC fully supports the views expressed by these organizations and strongly recommends against the adoption of Freedom of Information Act amendments that are so clearly counter-productive as the public faces growing concerns about cybersecurity.

B. The Proposed Cybersecurity Act of 2012

The proposed Cybersecurity Act of 2012 contains an Exemption Three provision in order to exempt from disclosure "any cybersecurity threat indicator disclosed by a non-Federal entity to a cybersecurity exchange."[29] The definition of "cybersecurity threat indicator" largely resembles that of "cyber threat information"

---

[26] SECURE IT Act of 2012, *supra* n. 25 at § 105.
[27] *Id.* at § 102(c)(4).
[28] *Id.* at § 101 (5); *see also* Elinor Mills, *Civil Liberties Groups: Proposed Cybersecurity Bill Is Too Broad*, CNET NEWS (Feb. 23, 2012), *available at* http://news.cnet.com/8301-27080_3-57384137-245/civil-liberties-groups-proposed-cybersecurity-bill-is-too-broad/ (as described below, the definition of "cybersecurity threat information" largely mirrors the definition of "cyber threat indicator" found in the Cybersecurity Act of 2012.
[29] Cybersecurity Act of 2012, *supra* n. 25 at § 704(d).

in the SECURE IT Act.[30] In order to prevent abuse of discretion, the implementation of both definitions would have to be subject to public scrutiny and oversight, the exact mechanisms the Freedom of Information Act exemptions would prevent.

The original purpose of Exemption Three was to provide for the continued use of non-disclosure or confidentiality provisions already included in other statutes. The Sunshine in Government Initiative estimates that over 240 Exemption Three statutes are currently active in federal law, and that each year federal department and agencies citing to "roughly 140 statutes to deny thousands of requests for information."[31]

V. EPIC, NSA, and the Freedom of Information Act: The Agency Remains a "Black hole" for Public Information about Cybersecurity

Over the years, EPIC has pursued numerous Freedom of Information Act matters with the NSA. We have done this because the NSA has played an increasingly significant role in domestic communications security. While we respect the technical expertise of the Agency, we also believe that it is vitally important that the NSA, like all federal agencies, remain accountable to the American public, particularly now that the agency has directed its extraordinary listening and processing capabilities to the private communications of the American public.

Between January 2009 and the hearing today, EPIC has pursued seven Freedom of Information Act requests with the NSA, concerning the NSA's cybersecurity operations. In six of those cases, the NSA has never disclosed documents responsive to EPIC's request. The NSA continually ignored the Freedom of Information Act's statutory deadlines or improperly refused to comply with required procedures. The NSA's actions in response to legitimate requests under the Freedom of Information Act have been evasive and egregious.

Of greatest significance, the agency has failed to provide documents to the public that are subject to disclosure under the Freedom of Information Act.

A. EPIC's FOIA Request for National Security Presidential Directive 54

The NSA has refused to release to the public even the Agency's legal basis, established by former President George W. Bush, which grants the authority for the NSA to conduct cybersecurity operations within the United States.

On June 25, 2009, EPIC submitted a Freedom of Information Act request to the NSA asking National Security Presidential Directive 54 (NSPD 54). NSPD 54 grants the NSA

---

[30] *Id.* at § 708(6). For concerns on this definition, *see Civil Liberties Groups: Proposed Cybersecurity Bill is Too Broad, supra* note 28.

[31] *See* National Academy of Public Administration: Open Government Dialogue, *The Administration Should Curb New Exemptions From FOIA*, http://opengov.ideascale.com/a/dtd/The-administration-should-curb-new-exemptions-from-FOIA/3194-4049 (last visited Mar. 9, 2012).

broad authority over the security of American computer networks. The Directive created the Comprehensive National Cybersecurity Initiative (CNCI), a "multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks." Neither NSPD 54 nor the CNCI has ever been released in whole.

Senators had previously noted that efforts to "downgrade the classification or declassify information regarding [CNCI] would...permit broader collaboration with the privacy sector and outside experts."[32] Only after EPIC filed a lawsuit against the NSA for their mishandling of EPIC's Request did the White House release a partially de-classified version of the CNCI. Among other things, the released version of the CNCI set forth EINSTEIN 3, the government's effort to conduct "real-time packet inspection" of all government Internet traffic.[33]

Although EPIC has still not received NSPD-54, we believe it is vitally important that the NSA provide to the public, at a minimum, the legal basis of its authority to conduct cybersecurity within the United States. As we have repeatedly stressed in our filings, we simply cannot accept a doctrine of "secret law" in the United States for such a critical government function.

B. EPIC's FOIA Request for the Testimony of Lieutenant General Keith Alexander

On April 16, 2010, EPIC requested from the NSA the "classified supplement" of Lieutenant General Keith Alexander, containing his answers to questions posed by the Senate Armed Service Committee in a hearing on his nomination to the position of NSA Director and Chief of the Central Security Service and Commander of the United States Cyber Command (CYBERCOM).

Much of Lieutenant General Alexander's public testimony raised questions about the growing influence of the military in civilian cybersecurity efforts, including an emphasis on the need to "be prepared to provide military options...if our national security is threatened."[34] When asked about the deployment of classified methods of monitoring electronic communications, most of the Lieutenant General's response was classified. Despite the notable public interest in the practice of monitoring Internet traffic, the NSA has again refused to make this information available to the public.

C. EPIC's FOIA Requests Cybersecurity Risk Assessments

---

[32] Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

[33] WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[34] Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command (Unclassified), *available at* http://senate.gov/~armed_services/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

The NSA has also locked relationships and agreements with private industry away. Under the National Strategy to Secure Cyberspace, the NSA was given the authority to provide technical assistance to owners of national security systems and conduct vulnerability assessments of those systems and disseminate information on threats to and vulnerabilities of national security systems.[35] Reports have confirmed the NSA's role in providing risk assessments to private industry.[36]

EPIC requested from the NSA all policies and procedures used to conduct vulnerability assessments or penetration tests on private networks. [37] Despite the White House's acknowledgement of the value of public participation in the cybersecurity process, again no documents were disclosed.

D. EPIC's FOIA Request for NSA Internet Wiretapping

In 2010, the NSA was developing new regulations, in cooperation with the Federal Bureau of Investigation and the Department of Justice, in order to require "all services that enable communications – including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook, and software that allows direct 'peer to peer' messaging like Skype – to be technically capable of complying if served with a wiretap order."[38]

EPIC requested the text of this proposal in order to educate the public on the issue in light of its upcoming submission to Congress and its imminent far-reaching impact on all Internet users. Despite a request for expedited treatment, the NSA has not yet disclosed any documents in response to EPIC's request.

E. EPIC v. NSA: The NSA-Google Cybersecurity Relationship

On January 12, 2010, Google reported that the company had suffered a "highly sophisticated and coordinated" cyber attack originating from China. The attackers planted malicious code in Google's corporate networks, and resulted in the theft of Google's intellectual property, and at least the attempted access of the Gmail accounts of Chinese human rights activists. The following day, Google changed a key setting, causing all subsequent traffic to and from its electronic mail servers to be encrypted by default. On

---

[35] Dept. of Homeland Security, The National Strategy to Secure Cyberspace, *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (2003).
[36] Ellen Nakashima, *Google to Enlist NSA to Help It Ward off Cyberattacks*, Wash. Post., Feb. 4, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR1010020304057.html.
[37] Executive Office of the President, Cyberspace Policy Review (2009) at C-7 n. 28, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf ("People cannot value security without first understanding how much is at risk.").
[38] Charlie Savage, *U.S. Tries to Make it Easier to Wiretap the Internet*, New York Times, Sept. 27, 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&ref=technology; Ellen Nakashima, *U.S. Seeks Ways to Wiretap the Internet*, Washington Post, Sept. 28, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706637.html.

February 4, 2010, the Washington Post reported that Google had contacted the National Security Agency ("NSA") regarding the firm's security practices immediately following the attack. In addition, the Wall Street Journal stated that the NSA's general counsel had drafted a "cooperative research and development agreement" within 24 hours of Google's announcement of the attack, which authorized the Agency to "examine some of the data related to the intrusion into Google's systems."

EPIC submitted a Freedom of Information request to the NSA requesting documents that pertained to the relationship between the NSA and Google. The NSA responded to EPIC's Freedom of Information Act request by issuing a Glomar response – refusing to confirm or deny that records existed. The NSA broadly defined their authority to operate secretly to an unprecedented degree, claiming that it was not even necessary to search for documents before making a substantive decision on what those documents may contain.

The NSA's claims would allow the agency to exercise unfettered discretion to dismiss any Freedom of Information request brought before it. For this reason, EPIC will be arguing before the DC Circuit next week in support of the public's right to know about the cyber security decisions that may determine, for example, whether a federal agency believes individual users should routinely encrypt their email.

F. ThinThread and Trailblazer

Even when the NSA publicly announces a surveillance program, the Agency's procedures under the Freedom of Information Act have shielded key documents from the public. As far back as 2000, the NSA implemented surveillance programs code-named ThinThread and Trailblazer in order to collect large quantities of data from various sources – financial transactions, travel records, web searches, and GPS equipment.[39] The pilot program, ThinThread, was abandoned in 2000 due to concerns of legality, and replaced by Trailblazer.[40] After having received a request from EPIC for contracts, agreements, and technical specifications regarding how information was gathered and used under the programs, the NSA failed to produce responsive.

The NSA's failure to provide information to the public about these programs may have also undercut efforts to promote cyber security in the United States.

G. EPIC FOIA Request for the NSA's "Perfect Citizen" Program

In 2010, the NSA recently completed a contract to develop "a set of sensors deployed in computer networks for critical infrastructure that would be triggered by

[39] Siobhan Gorman, *NSA Killed System That Sifted Phone Data Legally*, The Baltimore Sun, May 18, 2006, *available at* http://www.baltimoresun.com/news/nationworld/bal-nsa517,0,5970724.story?coll=bal-home-headlines.
[40] *Id.*

unusual activity suggesting an impending cyber attack."[41] The company that the NSA was contracting with, Raytheon, described the program as "Big Brother."[42] The program was to be funded as part of the CNCI, the White House's cybersecurity plan that the NSA refused to release in full to the public under a separate EPIC FOIA request.[43] EPIC has requested, but not received, the contracts under which the program was formed and any analyses or legal memoranda related to it.

The NSA's practices in response to requests for information under the Freedom of Information Act paint a picture of an Agency shrouded in secrecy that refuses to disclose even documents that are demonstrably vital to facilitating public involvement in the cybersecurity. The broad assertion of Section 6 of the NSA Act, the agency's Exemption Three statute for Freedom of Information Act purposes, is a reminder of what government agency's do with secrecy: they keep the public in the dark even as their own programs flounder and fail.

EPIC's experience over the last several years trying to obtain relevant information from the NSA concerning cybersecurity activities that directly impact the American public is a clear warning about the dangers of government secrecy. We strongly urge the Congress to maintain its vigorous defense of openness and agency accountability. While it may be tempting to establish new forms of government secrecy to respond to new threats, those changes are more likely to cause new problems than to offer workable solutions.

Thank you for your consideration of our views. We will provide additional information as it becomes available.

Sincerely,

/s/
Marc Rotenberg
EPIC Executive Director

/s/
Ginger McCall
Director, EPIC Open Government Project

/s/
Amie Stepanovich
EPIC National Security Counsel

---

[41] Siobhan Gorman, *U.S. Program to Detect Cyber Attacks on Infrastructure*, Wall St. J., July 8, 2010, *available at* http://online.wsj.com/article/SB10014240527487045450045753529838504 63.html.
[42] *Id.*
[43] *See supra* pp. 7-8.

Testimony of:
J. M. Ensminger
[redacted]
Elizabethtown, N. C. 28337
Email: [redacted]
Phone: [redacted]

Good morning, I would like to thank the chairman and the ranking member for offering me this opportunity to appear here today. I am here to testify on why access to information through FOIA matters to me and others from Camp Lejeune and about the extreme secrecy we have encountered in trying to expose the truth.

My name is Jerry Ensminger and I served my country faithfully for 24 years in the United States Marine Corps. My daughter Janey, the only one of my four children to be conceived, carried, or born while living aboard Camp Lejeune was diagnosed with leukemia in 1983 at the age of six. Janey went through hell and all of us who loved her went through hell with her. I watched my daughter die a little bit at a time for nearly 2 ½ years before she finally lost her fight. The leukemia won. Janey died on 24 September 1985.

Shortly after Janey's diagnosis, I began to wonder why. Why was she stricken with this disease? I researched mine and her mother's family histories and I could find no other child that had been diagnosed with leukemia or any type of cancer. It wasn't until August of 1997, three years after I had retired from the Marine Corps that I heard of a report indicating that the drinking water at Camp Lejeune had been contaminated during the time we lived there with chemicals suspected of causing childhood cancers and birth defects. That was the beginning of my journey on a search for answers and the truth. Little did I realize how difficult it would be getting the truth out of an organization which supposedly prides itself on honor and integrity!

None of what I'm about to say is speculation. It is all facts which are borne out by the Department of the Navy (DON) and United States Marine Corps (USMC) own documents. Throughout the history of this situation and to this very day, representatives of the DON/USMC have knowingly provided investigating/studying agencies with incorrect data, they have omitted data, they have obfuscated facts, and told many half-truths and total lies. They had DON/USMC contractors create a password protected electronic portal where they stashed all of the information/data pertaining to the massive gasoline pollution in the ground near drinking water supply wells. The Agency for Toxic Substances and Disease Registry (ATSDR) began their work at Camp Lejeune in 1991. They inadvertently uncovered the existence of this password protected electronic portal in 2009.

The DON/USMC's latest attempt to block the truth and foil justice is being done by defining key information being utilized by the ATSDR in their study reports concerning the base's contaminated tap water as "critical infrastructure information" or CII. They also slapped a label of "FOR OFFICIAL USE ONLY" (FOUO) on all documents relating to the contamination. Most of these documents and information they are labeling CII have been in the public domain for more than a decade and some for nearly 50 years. Mr. Chairman, the ATSDR estimates that as many as 1 million people were exposed to horrendous levels of carcinogenic chemicals through their drinking water at Camp Lejeune. These people need the uncensored truth concerning their exposures so they can be more vigilant about their and their family's health.

The United States Marine Corps, in their public statements, claim that they are working with the ATSDR and supporting ATSDR's efforts to answer the questions being asked by the exposed population. The only problem with that statement is that behind the scenes activities by DON/USMC aimed at subverting and undermining ATSDR's studies belie their words! The most recent attempt by the DON/USMC to suppress the public's knowledge

regarding ATSDR's Camp Lejeune studies came on 5 January of this year in the form of a letter (Encl.) from the USMC to the ATSDR. Without any public interest balancing test having been executed, key information was redacted from a critical report which experts are now saying will greatly diminish its scientific value/credibility (Encl.). This was labeled CII by the DON/USMC, but the legal justifications they cited for requesting these redactions were dubious at best. They notably did not mention the new law now governing what ultimately can be withheld from the public under the Freedom of Information Act by DoD to protect CII which was signed into law last December in the National Defense Authorization Act (NDAA) for Fiscal Year 2012.

It has also been reported that the ATSDR is currently in the process of "scrubbing" their Camp Lejeune website of key data/information published in previously released reports. This is all being done without any consideration of the public's need, interest, or right to know. For many of the exposed Camp Lejeune population, this information could literally mean life or death.

Mr. Chairman, the last thing we need is more secrecy disguised as a concern for the security of critical infrastructure. Any exemption must be very narrowly defined as it is in the new CII FOIA exemption for DOD. There must be an enforced public interest balancing test to ensure that any security interests outweigh other public interests—like health and safety, and there must be adequate reporting and oversight on how the exemption is used.

I want to thank Chairman Leahy and Representative Maloney for narrowing the blanket exemption to FOIA for critical infrastructure information that DOD was seeking in the National Defense Authorization Act for Fiscal Year 2012. Now all we need is oversight to ensure the law is implemented and followed! The hearing to day is a good start! Thank you.

Enclosures (7)

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5000
LF
JAN 5 2012

Dr. Thomas Sinks
Deputy Director
National Center for Environmental Health/
Agency for Toxic Substances and Disease Registry
4770 Buford Highway, NE
Atlanta, GA 30341

Dear Dr. Sinks:

Over the years force protection vulnerabilities have been unintentionally created in some Camp Lejeune products, to include the upcoming Chapter B report. The purpose of this letter is to request your assistance to mitigate security risks involved in this situation.

In the years since your agency began working on Camp Lejeune drinking water research initiatives, the security environment has significantly changed and there is now a greater need to provide robust and effective force protection for Marines, Sailors, civilian employees and their families who live or work aboard our bases and installations. Force Protection includes not only physical protection measures (e.g., gates and fences), but also measures to protect the security of sensitive asset and infrastructure information (e.g., water systems information).

Broad force protection efforts to identify vulnerabilities are ongoing across the Marine Corps and the other services. The attached page includes a synopsis of some of the governing regulations.

Recognition that these force protection concerns intersected with information contained in your Camp Lejeune reports first arose during a July 2010 Data Mining Technical Workgroup meeting held at Camp Lejeune. In August 2011, the new commander at Camp Lejeune requested a security review of the type of information that was included in previous water modeling reports. This security review concluded that the release of some of the specific information pertaining to active drinking water systems aboard Camp Lejeune potentially places those who live or work aboard the base at risk.

Our respective staffs discussed these issues and the conclusions from the security review. Your staff rightly requested references to assist their understanding and to provide concise guidance about release of sensitive water system information into the public domain.

I know that some sensitive information has already been released into the public domain in such places as some Marine Corps and other government agency websites. Changing security threats and evolving

Encl. (1)

policy, however, compel us to continuously evaluate information available in the public domain. To that end, I request that we work together to review our public domain materials and take appropriate steps to protect critical infrastructure information.

More specifically, after consulting with our security experts, I have provided the following guidance to my staff. I encourage you to provide this information to your staff, too:

1) Review new information carefully to avoid releasing location information for active potable water wells, raw or treated potable water lines, water treatment plants or water storage tanks which may not be released to the public in coordinate, map, or other form.

2) Review information on active potable water wells, raw or treated potable water lines, water treatment plants or water storage tanks that have been released in the past and, to the extent possible, remove that information from existing web sites.

3) Release without restriction, where and when otherwise appropriate, the location information for inactive or demolished potable water wells or non-potable monitoring wells in coordinate, map, or other form.

The Marine Corps understands the need to share information with the scientific community. Prudence requires, however, that information sharing be within the rubric of responsible force protection. I greatly appreciate your cooperation and look forward to working with you in this on-going effort to protect our forces and families.

Sincerely,

J. A. KESSLER
Major General
Assistant Deputy Commandant
Installations and Logistics
(Facilities)

Attachment
References to Protection of
Critical Assets

Encl (1)

References to Protection of Critical Assets

DoDI 2000.16: Department of Defense (DoD) Instruction 2000.16 (DoD Antiterrorism Standards) requires DoD components to identify critical assets, and subsequently develop and implement risk mitigation measures to reduce the vulnerabilities of DoD critical assets (e.g., water distribution infrastructure). Since July 2010, the Marine Corps has been conducting Mission Assurance Assessments on its bases and installations in order to identify and formally catalog all of our critical assets and infrastructure. Our consolidated Mission Assurance/All Hazards Risk Assessment Program integrates all aspects of Mission Assurance to include the identification of assets and infrastructure critical to mission execution. After the completion of these assessments, the Marine Corps will publish a policy document that addresses specific actions that will be taken to reduce risk and ensure the protection of our personnel and infrastructure.

U.S. Code Title 18, PART I, CHAPTER 37, Sec. 795 (a): "Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information relative thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installations or equipment without first obtaining permission of the commanding officer of the military post, camp, or station, and any separate military or naval command concerned, or higher authority, and promptly submitting the product obtained to such commanding officer or higher authority for censorship or such other action as he may deem necessary." Further, Exemption 9 of the Freedom of Information Act (FOIA) broadly exempts disclosure of information pertaining to "geological and geophysical information and data, including maps, concerning wells."

SECNAV M-5510.36 requires that "a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on publicly accessible websites or computer servers."

SECNAV M-5510.36, Department of the Navy Information Security Program Chapter 8: requires commanders to safeguard information pertaining to critical assets and infrastructure.

On 22 April 2011, the Commandant of the Marine Corps published guidance to all commanding Generals, all Commanding Officers, and All Officers in Charge on Information Protection. In that "White Letter" the Commandant directed a range of actions to improve operational security and protection of sensitive information and IT systems.

Encl (1)

Congress of the United States
Washington, DC 20515

January 27, 2012

Dr. Thomas R. Frieden,
Director, Centers for Disease Control and Prevention
Administrator, Agency for Toxic Substances and Disease Registry
1600 Clifton Rd
Atlanta, GA 30333

Dear Dr. Frieden,

We have been following with great interest the progress of studies being conducted by the Agency for Toxic Substances and Disease Registry (ATSDR) on the effects of water contamination at Marine Corps Base Camp Lejeune, North Carolina. Recently, we were made aware of a letter from the United States Marine Corps (USMC) to ATSDR regarding concerns about the content of ATSDR's Chapter "B" report and "force protection vulnerabilities" for Camp Lejeune's infrastructure the USMC claimed might be at risk if information in the report was not redacted. The USMC letter raises several serious questions and concerns that we believe warrant your timely attention.

The men and women who served at Camp Lejeune are seeking answers to questions about how they were affected by contaminated drinking water. An open and transparent process is essential to this scientific endeavor and it is particularly important for the ongoing and future studies on Camp Lejeune's water contamination. Without an open and transparent process, questions about the validity of the ATSDR studies could be raised in the future. The USMC's most recent concerns regarding these studies - conveyed in writing only days before the Chapter "B" report was to be released - have raised serious questions about the legal basis for their claims of force protection vulnerabilities. As you know, the Department of Navy's history of withholding statutorily required funding for ATSDR's studies and their past lack of cooperation and transparency in providing all necessary data to ATSDR have not been viewed favorably by Congress. This most recent request from the USMC to ATSDR asking ATSDR to redact portions of a statutorily required report has only heightened our concerns.

We are aware that ATSDR released Chapter "B" of the Hadnot Point-Holcomb Boulevard Reports on January 19, 2012 and did so after agreeing with the Marine Corps that redacting the current locations of Camp Lejeune's active installation water system infrastructure was in the public's interest due to national security concerns. We were told by ATSDR that your agency determined the redactions of this information will have no effect on the conclusions contained in the report or on a lay reader's understanding of the report. However, we remain concerned that these redactions may have established a legal precedent for withholding information from scientific studies for reasons of national security without adequate legal justification that the information pertains to "critical infrastructure" or "sensitive information" that is excluded by current law.

Encl (2)

Dr. Frieden
Page 2

We specifically question whether the USMC's request to redact this information and ATSDR's acquiescence are legally sound, as Congress has not prohibited the release of this information in the past, the information has not been classified as falling under a FOIA exemption, and the information has been publically available for several years. For these reasons, we would like a response from your agency to the following questions:

1. When did General Counsel from ATSDR or the Centers for Disease Control (CDC) receive the January 5, 2012 letter from the USMC and when was the USMC notified that ATSDR had found the legal basis for the USMC's request to be legally valid? On what grounds of legal determination and justification was the request found to be valid? Did ATSDR staff provide any assurances to USMC that the USMC's concerns stated in the letter would be agreed to, prior to ATSDR's receipt of the letter?
2. Did ATSDR or CDC counsel confer with their counterparts in the USMC, Department of Navy, or Department of Defense before validating the letter's legal justifications under Department of Defense internal instructions and FOIA Exemption 9 and, if so, was there any discussion of the ramifications and implications of redacting information not previously found to be "critical infrastructure" or "sensitive information" under the law?
3. Are there codified procedures, besides interagency Memorandums of Understanding, that have been used by ATSDR and/or CDC for past ATSDR studies containing unclassified, but potentially sensitive information, to determine if that information should or should not be withheld from the public? If so, please provide a copy of those procedures and advise us if they were applied and followed in this case? If they were not applied and followed, would those procedures apply in this case and why or why not?
4. What determination has been made by ATSDR or CDC that withholding the information redacted from Chapter "B" will not render the report invalid by peer reviewers and on what was that determination based?
5. In addition to peer review, did your agency also consider potential longer term ramifications from this most recent decision to redact information, to the extent it may encourage future requests from Department of Defense to redact information in the public's interest by invoking a national security concerns or adversely affect future FOIA requests from the public?

We appreciate your attention to this important matter and look forward to your response. Given the significance of the issues we have raised, we request an official response be provided to our offices no later than February 17, 2012.

Sincerely,

Senator Richard Burr | Representative Brad Miller | Representative John Dingell

Senator Bill Nelson | Senator Marco Rubio | Senator Kay Hagan

Encl (2)

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Public Health Service

Centers for Disease Control
and Prevention (CDC)
Atlanta GA 30333

February 15, 2012

The Honorable Brad Miller
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Miller:

Thank you for your letter regarding the Agency for Toxic Substances and Disease Registry's (ATSDR) investigations at United States Marine Corps Base Camp Lejeune (Camp Lejeune). Your ongoing support of our Camp Lejeune investigations has allowed us to move forward in a scientifically comprehensive and valid manner. I have addressed your concerns below, and enclosed answers to your specific questions.

Please be assured that we are fully committed to maintaining an open and transparent process in our work at Camp Lejeune. ATSDR has developed feasibility assessments, study protocols, and study reports for its investigations and water modeling of Camp Lejeune volatile organic compound contamination in drinking water. ATSDR has subjected these plans and reports to review by experts outside the agency and the affected public using expert panels, peer review, and a Community Assistance Panel (CAP). The CAP sessions are open to the public and are live streamed on the internet. The ATSDR website hosts detailed information, meeting notes, and Camp Lejeune reports. We have not altered our efforts to ensure transparency and openness, and will not do so. If the United States Marine Corps (USMC) attempts to compromise our work or its transparency, we will invoke the dispute clause included in our memorandum of understanding with the Department of Navy (DON).

As you mentioned, on January 5, 2012, ATSDR received a letter from the USMC/DON raising installation security concerns at Camp Lejeune if certain information was published. The letter asked that we "*Review new information carefully to avoid releasing location information for active potable water wells, raw or treated potable water lines, water treatment plants with water storage tanks which may not be released to the public in coordinate, map, or other form.*" On January 19, 2012, ATSDR released a report titled *Chapter B: Geohydrologic Framework of the Brewster Boulevard and Castle Hayne Aquifer Systems and the Tarawa Terrace Aquifer*. In keeping with the USMC request, ATSDR redacted longitude and latitude coordinates of active drinking water infrastructure from the report.

The security of military personnel and installations is a serious matter. ATSDR does not have the expertise to evaluate installation security at Camp Lejeune and cannot agree or disagree with the USMC that locations of active installation water system infrastructure are a national security concern. We made the limited redactions to the document because including the longitude and latitude coordinates of active drinking water infrastructure was scientifically unnecessary for the purpose of the document. The redactions are consistent with a U.S. Environmental Protection

Encl (3)

Agency (EPA) position related to security risks of active public drinking water infrastructure.[1] EPA has concluded that it is prudent to restrict from public dissemination the latitude and longitude coordinates of well intakes, source water areas, and source water assessment program data. Redacting the document allowed us to balance the USMC base security concerns with our public health mission and resulted in the release of Chapter "B" within days of receiving the USMC letter from Major General Kessler. Since the redactions in the report were not made in response to a Freedom of Information Act request, ATSDR did not review in detail the legal basis for the USMC claims of force protection vulnerabilities. ATSDR has recently received a Freedom of Information Act (FOIA) request for the Chapter "B" information. Prior to making a final determination regarding redacting the longitude and latitude coordinates in accordance with the FOIA, ATSDR will consult with USMC/DON and review in detail the legal basis for USMC's claims of force protection vulnerabilities, pursuant to FOIA and Department of Health and Human Services regulations.

We greatly appreciate your leadership and assistance with the ATSDR Camp Lejeune investigations and are committed to completing these investigations in an open, timely, and transparent manner using the best science available to us. If you have any additional questions about the Camp Lejeune investigations, please feel free to contact Dr. Richard Weston in the Centers for Disease Control and Prevention's (CDC) Washington office at rtw8@cdc.gov or (202) 245-0600. The cosigners of your letter will also receive this response.

Sincerely,

Thomas R. Frieden, M.D., M.P.H.
Director, CDC, and
Administrator, ATSDR

Enclosure

[1] April 4, 2005: *Policy to Manage and Access to Sensitive Drinking Water Related Information.* USEPA, Office of Water.
http://water.epa.gov/infrastructure/watersecurity/lawsregs/upload/policytomanageaccesstosensitivedwrelatedinfoApril2005.pdf

Encl (3)

ATSDR Chapter "B" – Responses to Questions posed to Dr. Thomas Frieden

1. *When did General Counsel from ATSDR or the Centers for Disease Control (CDC) receive the January 5, 2012 letter from the USMC and when was the USMC notified that ATSDR had found the legal basis for the USMC's request to be legally valid? On what grounds of legal determination and justification was the request found to be valid? Did ATSDR staff provide any assurances to USMC that the USMC's concerns stated in the letter would be agreed to, prior to ATSDR's receipt of the letter?*

   The CDC/ATSDR Office of General Counsel received a copy of the letter on January 5, 2012. Although we were aware of USMC's concerns prior to receiving this letter, we did not provide assurances to DON that we would agree to the USMC concerns before January 5, 2012.

   The DON and CDC/ATSDR Offices of General Counsel initially discussed the issue of sensitive installation drinking water infrastructure during the summer of 2010. At that time, we did not identify a legal basis for defining the type or extent of information required to be released or withheld in an ATSDR document and the issue was referred back to appropriate program officials for further review. DON first defined the information they considered sensitive during a video conference call with ATSDR on December 9, 2011. We responded by e-mail stating "*While we are evaluating [your] concerns, we will not alter our reports until we receive specific requests we can act upon in writing.*"

   We take the security of military personnel and installations very seriously. ATSDR does not have the expertise to evaluate installation security at Camp Lejeune and we are not in a position to agree or disagree with the USMC that locations of active installation water system infrastructure are a national security concern. We made the limited redactions to the document because including the longitude and latitude coordinates of active drinking water infrastructure was scientifically unnecessary for the purpose of the document. We have not made a determination that USMC's request is legally valid.

2. *Did ATSDR or CDC counsel confer with their counterparts in the USMC, Department of Navy, or Department of Defense before validating the letter's legal justifications under Department of Defense internal instructions and FOIA Exemption 9 and, if so, was there any discussion of the ramifications and implications of redacting information not previously found to be "critical infrastructure" or "sensitive information" under the law?*

   CDC/ATSDR counsel did not confer with USMC, DON, or DOD counterparts about the letter before we released the redacted version of Chapter "B." We follow FOIA procedures when releasing information requested by the public under FOIA. The release of this report, however, was not in response to a FOIA request, but part of ATSDR's public health work at the site. We are continuing to work with DON to address issues of disclosure of information that may impact installation security while preserving the integrity and transparency of our activities. ATSDR has recently received a FOIA request for the Chapter "B" report, including the redacted drinking water infrastructure information, i.e., the well longitude and

Encl (3)

latitude coordinates. Prior to making a final determination regarding redacting the longitude and latitude coordinates in accordance with the FOIA, ATSDR will consult with USMC/DON and review in detail the legal basis for USMC's claims of force protection vulnerabilities, pursuant to FOIA and Department of Health and Human Services regulations.

3. *Are there codified procedures, besides interagency Memorandum of Understanding, that have been used by ATSDR and/or CDC for past ATSDR studies containing unclassified, but potentially sensitive information, to determine if that information should or should not be withheld from the public? If so, please provide a copy of those procedures and advise us if they were applied and followed in this case? If they were not applied and followed, would those procedures apply in this case and why or why not?*

   We are not aware of any codified procedures specific to ATSDR studies. Our memorandum of understanding with DON includes a dispute clause, which we will not hesitate to invoke if we feel that USMC is attempting to compromise our work or its transparency. We are committed to our public health mission and have not altered our efforts to ensure transparency and openness, nor will we do so.

4. *What determination has been made by ATSDR or CDC that withholding the information redacted by Chapter "B" will not render the report invalid by peer reviewers and on what was that determination made?*

   ATSDR documents go through an internal and external peer review process before they are released to the public. Peer reviewers analyzed an unredacted draft of Chapter "B," which was the basis for the review comments they provided to ATSDR. Following the peer review and subsequent suggested redaction, all involved ATSDR staff agreed that including detailed geographic locations of active drinking water infrastructure was not scientifically necessary for the purpose of this document and that the redactions would not diminish its scientific integrity.

5. *In addition to peer review, did your agency also consider potential longer term ramifications from this most recent decision to redact information, to the extent it may encourage future requests from the Department of Defense to redact information in the public's interest by invoking national security concerns or adversely affect future FOIA requests from the public?*

   Using the 2005 EPA memorandum as a guide, we are developing a policy on managing and accessing sensitive drinking water related information to ensure a long-term resolution of this issue. We are committed to following FOIA procedures and will invoke the dispute resolution in our memorandum of understanding with DON if we disagree on an issue, including national security concerns. Please be assured that the issue of base security does not affect how we conduct our work to determine human health risks from exposures to historic contaminated drinking water at Camp Lejeune.

Encl (3)

Christopher J. Portier, Ph.D.
Director, NCEH/ATSDR
4770 Buford Highway, N.E
Building 106, Mail Stop F-61
Atlanta, Georgia 30341-3717

February 19, 2012

Dear Dr. Portier:

As the Hydrologist/Civil Engineer under contract to Eastern Research Group, Inc. (ERG), I am the sole author of ATSDR's Hadnot Point-Holcomb Boulevard Chapter B report, herein referred to as Chapter B. Oversight and review of Chapter B was provided by Mr. Morris L. Maslia, Project Officer for all of the ATSDR Camp Lejeune water-modeling activities. The purpose of my letter to you is to point out specific misleading statements in Dr. Frieden's letter of February 15, 2012, wherein he replies to the several Senators and Congressmen who questioned ATSDR's redaction of well coordinate data from the publicly released version of the Chapter B report.

I thought Dr. Frieden's letter was informative and generally to the point. However, several statements in Dr. Frieden's letter that comment on the scientific content of Chapter B are false and misleading. As the author of Chapter B, I consider it my ethical and professional responsibility to inform you of these misleading statements and I retain the hope that, at some future time, CDC/ATSDR will inform Congress of same.

The second sentence of paragraph 4 (page 1) of Dr. Frieden's letter states that "*We (ATSDR) made the limited redactions to the document (Chapter B) because the longitude and latitude coordinates of active drinking water infrastructure was scientifically unnecessary for the purpose of the document*".

This sentence is patently false on its face and, from a scientific point-of-view, borders on the inane and silly. The quoted statement also implies that an unprofessional or unethical endeavor was somehow in effect during the writing of Chapter B. Why would well coordinate data be included in the Chapter B report if not to support and document the scientific results and interpretations published therein?

Because well coordinate (control point) data were redacted from tables used to construct most of the top and thickness maps published in Chapter B, any attempt to reproduce the published maps using just the publicly released data would result in failure. Such failures would be increasingly pronounced with increasing depth of occurrence of the particular geohydrologic unit. For example, consider the map and related control point data for the Upper Castle Hayne aquifer-River Bend unit, a major water-bearing unit for supply wells in the study area (Figure B17, Table B15). Fully **33 percent** of the control points used to create Figure B17 were redacted from the publicly released version of Chapter B. Such deletions could not help but to change the published interpretations of the surface and

Encl (4)

thickness of this unit. Similar changes for similar reasons would accrue to the published results for the Middle Castle Hayne aquifer (Figure B25, Table B19), perhaps the most significant water-bearing unit for supply wells, where almost **50 percent** of the useful control point data were redacted. Redactions amounting to **33 percent** and **50 percent** of useful data are **NOT** the "*limited redactions*", as stated in Dr. Frieden's letter to Congress.

As you know, the geohydrologic unit control point data published in Chapter B were directly transferred, to the geohydrologic framework established for all Hadnot Point-Holcomb Boulevard groundwater-flow models. Thus, the redaction of well coordinate data from the publicly released version of Chapter B also significantly compromises any effort to reproduce the geohydrologic framework assigned to the project groundwater-flow models. These redaction issues, in my opinion, now call into question the reproducibility and scientific integrity of: (1) my analyses, (2) the Chapter B report in its entirety and (3) subsequent water-modeling reports for the Camp Lejeune historical reconstruction analyses.

In response to question #4 from the Congressmen and Senators (page 2?), Dr. Frieden's letter states that "*Following the peer review and subsequent suggested redaction, all involved ATSDR staff agreed that including detailed geographic locations of active drinking water infrastructure was not scientifically necessary for the purpose of this document (Chapter B) and that the redactions would not diminish its scientific integrity.*"

This statement is false and egregiously disingenuous, as I interpret it, or perhaps just poorly worded. Regardless, the uninformed reader is left with the impression that redactions of well coordinate (control point) data from Chapter B were a recommendation of the peer review process. As the author of Chapter B, I read and responded to **all** of the several peer review summaries regarding Chapter B, including those from Camp Lejeune and U.S. Navy personnel, and no peer reviewer ever recommended or even suggested that well coordinate data be redacted from the Chapter B report. (The ATSDR Project Officer, Mr. Morris Maslia, and the NCEH/ATSDR Deputy Director, Dr. Tom Sinks also reviewed all of the peer review summaries and my response to same in their entirety.)

In addition, the quote from Dr. Frieden's letter states that "*all involved ATSDR staff*" agreed with or supported a decision to redact well coordinate data from Chapter B. Although the verbiage "ATSDR Staff" is somewhat ambiguous and I am just the author of Chapter B and not an employee of ATSDR, I want to state for the record herein that, as a matter of professional ethics and common sense, I did and do totally disagree with ATSDR's policy decision to redact data. Furthermore, I believe that Mr. Morris Maslia, ATSDR's Camp Lejeune Project Officer, forcefully expressed this same opinion to you and other ATSDR policy makers.

Dr. Portier, I believe my comments in the previous paragraphs substantially contradict the parts of the quoted statement regarding scientific necessity and the notion that redactions would not "*diminish*" the scientific integrity of the Chapter B report. In summary, I

Encl (4)

strongly suggest that the redactions of well coordinate data, as evidenced in the publicly released version of Chapter B, do indeed **substantially compromise the technical and scientific integrity of Chapter B, and possibly, by extension, the results of the forthcoming water-model simulations**.

In passing, I note that well coordinate locations in Dr. Frieden's letter are consistently referred to in terms of latitude and longitude. Please note, that **ALL** well coordinate data in Chapter B are stated in North Carolina State Plane Coordinates, North American Datum of 1983. Even a casual reader of Chapter B would have realized that State Plane coordinates were the locators of choice. I am sure that if I or ATSDR's Camp Lejeune Project Officer had been given an opportunity to review the final draft of Dr. Frieden's letter for content and accuracy, this error would have been pointed out.

I hope these comments are helpful.

Sincerely,

Robert E Faye

Digitally signed by Robert Faye
DN: cn=Robert Faye, o, ou, email=refaye@windstream.net, c=US
Date: 2012.02.19 20:27:22 -05'00'

Robert E. Faye P.E. MSCE

copy to:

Dr. Thomas Frieden, Director, CDC
Mr. Morris L. Maslia, P.E., DEE, ATSDR Project Officer

Encl (4)

CAROLYN B. MALONEY
14TH DISTRICT, NEW YORK

2332 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-3214
(202) 225-7944

COMMITTEES:
FINANCIAL SERVICES

OVERSIGHT AND
GOVERNMENT REFORM

JOINT ECONOMIC COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–3214

DISTRICT OFFICES:

☐ 1651 THIRD AVENUE
SUITE 311
NEW YORK, NY 10128
(212) 860-0606

☐ 21-77 31ST STREET
ASTORIA, NY 11105
(718) 932-1804

WEBSITE: http://maloney.house.gov

February 24, 2012

The Honorable Leon E. Panetta
Secretary
U.S. Department of Defense
100 Defense Pentagon
Washington, DC 20301

Dear Mr. Secretary,

I write with great concern regarding recent reports of a Department of the Navy request to redact information from an Agency for Toxic Substances and Disease Registry (ATSDR) report about water contamination at the U.S. Marine Corps base, Camp Lejeune—where for three decades, thousands of Marines and their families consumed tap water contaminated with toxic chemicals that likely led to cancers and other illnesses, but have yet to receive justice.

I authored a provision that was included in the House-passed version of H.R. 1540, the National Defense Authorization Act for Fiscal Year 2012 that requires the application of a public interest balancing test by the Department of Defense (DoD) when exempting clearly-defined, sensitive, but unclassified "Critical Infrastructure Security Information," or CISI, from responses to Freedom of Information Act (FOIA) requests. As you know, the final, compromise language that was passed as part of the FY12 NDAA conference report, which was signed into law on December 31, 2011, would permit the withholding of CISI under the Freedom of Information Act (FOIA) only when the public interest is outweighed by the interests in security. This determination is to be made in writing by the Secretary of Defense, or designee, and then made public.

Given the documented history of secrecy surrounding the Camp Lejeune investigation, the Department of the Navy's actions raise serious concerns regarding the legal justifications for its most recent request for redactions from the Camp Lejeune report, particularly in light of the new CISI statutory exemption to FOIA. As you well know, ultimately all federal government information is public and available through a FOIA request unless classified or exempted through FOIA or the Privacy Act.

Certainly some CISI should not be made public due to security concerns interests that outweigh other public interests. However, all DoD components need guidance clarifying that CISI will only be truly secure if it can be properly be withheld under FOIA. Therefore, treatment of CISI should be governed by the DoD CISI exemption—not the host of other unrelated laws, regulations, and instructions cited by the Navy in its letter to ATSDR.

Encl (5)

I request that you provide the following information regarding the proper implementation of the new law:

- What measures is DoD undertaking to properly implement the use of the CISI exemption to FOIA?
- When does DoD plan to initiate the rulemaking process, and to clarify the appropriate usage of the exemption and how it may relate to existing instructions, regulations, or statutes relating to critical infrastructure information security?
- How will you ensure the public interest balancing test is appropriately and consistently applied and that requesters are given an opportunity to present the public interest in question once DoD has determined the requested information is CISI?
- How will DoD conduct oversight over the use of the CISI exemption?
- How will DoD ensure public access to determinations to withhold information using the CISI exemption?
- Finally, given the great public interest in information related to the Camp Lejeune water contamination, what measures are you taking to ensure that information is made publicly available?

We must protect certain CISI to keep our defense operations, properties and facilities safe from terrorists and others who would do harm to American interests. But in our efforts to do so, we also must strike the necessary balance between safeguarding security interests and the public's right to know – and prevent another Camp Lejeune from happening.

Thank you for your prompt attention to this matter, and I look forward to your reply.

Sincerely,

CAROLYN B. MALONEY
Member of Congress

Encl (5)

RICHARD BURR
NORTH CAROLINA

United States Senate
WASHINGTON, DC 20510
March 7, 2012

Daniel Levinson
Inspector General
Office of the Inspector General
U.S. Department of Health and Human Services
330 Independence Avenue, SW
Washington, DC 20201

Dear Inspector General Levinson:

I write today with concerns regarding the Agency for Toxic Substances and Disease Registry (ATSDR) decision to redact information from one of ATSDR's recent reports on the Marine Corps Base Camp Lejeune water contamination. ATSDR is issuing a series of reports this year as part of the battery of studies the agency has been collecting data for since 1991. These statutorily mandated studies are the culmination of decades of diligent and tireless scientific investigation by ATSDR into the largest human exposure to toxins on record at a domestic Department of Defense (DoD) installation. The hundreds of thousands of veterans and their families who lived at Camp Lejeune are anticipating that the ATSDR reports will provide them with the information they need to become informed about the scope and severity of the water contamination and educate them on the possible association between their exposures and current and future health effects.

On January 27, 2012, I and five other Members of Congress sent a letter to the Director, Centers for Disease Control and Prevention (CDC) asking for an explanation of ATSDR's decision to redact specific information from ATSDR's Hadnot Point-Holcomb Boulevard Chapter "B" Report (hereinafter referred to as "Chapter B") after the USMC sent a letter to ATSDR on January 5, 2012, that cited internal Department of Navy instructions and a Freedom of Information Act exemption as justification for this specific redaction. Dr. Frieden responded to the Congressional letter on February 15, 2012, and indicated that neither ATSDR nor CDC General Counsels had reviewed the legal rationale for the USMC's January 5, 2012, request and instead relied on Environmental Protection Agency (EPA) guidance in determining that the information could be redacted. Dr. Frieden further justified his decision by stating the redactions would not dilute or diminish the scientific merit or accuracy of Chapter B.

Since the redactions were made in Chapter B and the report was released in January, one of the two researchers responsible for Chapter B has formally disagreed with the decision by ATSDR leadership to redact a portion of the report and sent a letter to the ATSDR Director stating that

Encl (6)

the redactions removed specific data and information essential to the scientific process and conclusions within the report and "significantly compromises" the scientific value of the report (enclosed).

This issue is garnering significant attention in Congress and increasing in its urgency. Later this month, the Senate Judiciary Committee will hold a hearing to examine the issue of the Department of Defense (DoD) asserting various Freedom of Information Act (FOIA) exemptions to prevent public disclosure of what DoD refers to as "critical infrastructure/information" or CI/I. It is my understanding that the information redacted from Chapter B was not covered by the FOIA exemption cited by USMC, had not been formally identified by DoD as within CI/I, had already been available in the public domain for several years, and remains in the public domain on at least one government agency website and in reports published by government agencies.

I have the honor to serve as the Ranking Member of the Senate Veterans' Affairs Committee and as a member of the Senate Health, Education, Labor, and Pensions Committee, which has jurisdiction over ATSDR and CDC. Moreover, I take seriously my oversight responsibility of ensuring the transparency and integrity of our nation's public health programs and the agencies charged with investigating environmental exposure incidents and protecting the health of the American people, especially programs that have a direct impact on our nation's veterans and their families. Consequently, I am deeply troubled by the lack of formal legal review conducted prior to ATSDR's decision on redactions in Chapter B and I am concerned ATSDR may now be in the process of cooperating with DoD to redact information critical to public health from past, pending, and future Camp Lejeune reports. Therefore, I respectfully request that you investigate the prior and ongoing policies and practices at ATSDR and CDC with respect to the issues raised above. I further request that you examine the degree of formal and informal ATSDR and CDC communications with DoD, including Department of Navy and USMC representatives, regarding redactions of ATSDR reports on the Camp Lejeune water contamination in an effort to determine if the concerns I have raised have merit, and what, if any, actions should be taken by ATSDR and CDC to address these concerns.

Thank you in advance for your timely attention to this serious matter.

Sincerely,

Richard Burr
United States Senator

Enclosure: Letter from Robert E. Faye to Dr. Portier, ATSDR Director, dated February 19, 2012

Encl (6)

RICHARD BURR
NORTH CAROLINA

United States Senate

WASHINGTON, DC 20510

March 7, 2012

Dr. Thomas R. Frieden
Director, Centers for Disease Control and Prevention
Administrator, Agency for Toxic Substances and Disease Registry
1600 Clifton Rd
Atlanta, GA 30333

Dear Dr. Frieden,

I write out of continued concern regarding the integrity of the Agency for Toxic Substances and Disease Registry's (ATSDR) Camp Lejeune water contamination reports. I received your letter of February 15, 2012, regarding your decision to comply with a request from the United States Marine Corps (USMC) to redact public information from the Chapter "B" report based on USMC concerns about disclosure of "critical infrastructure/information" for reasons of national security. You stated that CDC and ATSDR General Counsels did not conduct any legal review of the USMC request before you agreed to redact this information from Chapter "B".

Your decision to redact that information has raised concerns about both the scientific integrity and merit of the report and its findings, as well as the Department of Defense's (DoD) role in this matter. As you are likely aware, the Senate Judiciary Committee will hold a hearing this month to look into the government's process for determining if information already made public, like that redacted from Chapter "B", is in fact "critical infrastructure/information" and should be withheld from future disclosure. One of your own researchers and the co-author of Chapter B has formally objected to the statements you made in your February 15 letter and raised significant questions about the internal process that led to those decisions (enclosure). I am concerned that ATSDR may be faced with additional requests from DoD to redact information from its reports on Camp Lejeune and that your decision on Chapter "B" may set an overly accommodative precedent with significant implications for the scientific integrity of the Chapter "B" report as well as future research based on this report's findings.

I met with you in 2010 to discuss the studies of water contamination at Camp Lejeune and the delays ATSDR was encountering to obtain funding from the Department of Navy (DoN) for those studies. I told you then that I would help ensure ATSDR was able to conduct and complete its studies unimpeded by the DoN. Those studies will be released this year and their scientific integrity is vital to the hundreds of thousands of veterans and their families waiting for answers. In an effort to ensure your agency is executing its mission properly and preserving the scientific integrity of these reports, I have requested that the Inspector General of the Department of Health

Encl (7)

and Human Services examine ATSDR's activities in this matter. I've taken this cautionary step because we are nearing a critical period in which the transparency, integrity, and ultimately the merit of the ATSDR reports will be essential to maintain the public's faith and confidence in the government's scientific process.

As the Administrator of ATSDR, you are personally responsible for the integrity of ATSDR's analysis and report on the Camp Lejeune water contamination. Therefore, before any pending or future reports on the Camp Lejeune water contamination are finalized and released this year, I would like you to personally assure me that all past, present, and future ATSDR reports on Camp Lejeune meet the highest standards of scientific completeness and credibility, that CDC or ATSDR is not prematurely deciding what information should be redacted from those reports for the sake of expediency at the behest of the Department of Defense, or one of its Service Components, and that any and all redactions approved and made by your agency have and will conform with legal precedent and the Freedom of Information Act.

Sincerely,

Richard Burr
United States Senator

Enclosure: Robert E. Faye letter to ATSDR Director, dated February 19, 2012

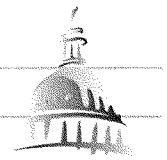
EnCL (7)

2

U.S. Senator Chuck Grassley • Iowa

Ranking Member • Senate Judiciary Committee

http://grassley.senate.gov



Statement of Senator Chuck Grassley of Iowa
Ranking Member, Senate Committee on the Judiciary
"The Freedom of Information Act: Safeguarding Critical Infrastructure Information and the Public's Right to Know."
Tuesday, March 13, 2012

Mr. Chairman, thank you for holding this hearing during Sunshine Week.

Open government and transparency are essential to maintaining our democratic form of government. Our Founding Fathers knew this, as James Madison once said -- "a people who mean to be their own governors must arm themselves with the power which knowledge gives."

The Freedom of Information Act codifies this fundamental principle which our Founders valued so dearly. So it's important to talk about the Act and the need for American citizens to be able to obtain information about how their government is operating.

Although it's Sunshine Week, I'm sorry to report that contrary to President Obama's proclamations when he took office, after three years, the sun still *isn't* shining in Washington, D.C.

Based on my experience in trying to pry information out of the executive branch, I'm disappointed to report that agencies under the control of President Obama's political appointees have been more aggressive than ever in withholding information from the public and from Congress.

There's a complete disconnect between the President's grand pronouncements about transparency and the actions of his political appointees.

On his first full day in office, President Obama issued a memorandum on the Freedom of Information Act. In it, he instructed executive agencies to

> "adopt a presumption in favor of disclosure, in order to renew their commitment to the principles embodied in FOIA, and to usher in a new era of open Government."

Unfortunately, it appears that in the eyes of the President's political appointees, his proclamations about open government and transparency -- are merely words, which can be ignored.

Indeed, FOIA requestors appear to have reached the same conclusion. For example, when recently asked about President Obama and FOIA, Katherine Meyer, an attorney who's been filing FOIA cases since 1978, said, that the Obama administration

> "is the worst on FOIA issues. The worst. There's just no question about it... This administration is raising one barrier after another. ... It's gotten to the point where I'm stunned — I'm really stunned."

The problem is more than just a matter of backlogs with answering FOIA requests. Based on investigative reports, we've learned of inappropriate actions by the President's political appointees.

In March of last year, two weeks after this Committee held a hearing on FOIA, the House Committee on Oversight and Government Reform released a 153-page report on its investigation of the political vetting of FOIA requests by the Department of Homeland Security. The committee reviewed thousands of pages of internal emails and memoranda and conducted six transcribed witness interviews.

The committee, under Chairman Issa, learned that political staff under Secretary Napolitano corrupted the agency's FOIA compliance procedures, exerted pressure on FOIA compliance officers, and undermined the federal government's accountability to the American people. The report's findings are disturbing. I'll just summarize four of them.

First, the report finds that by the end of September 2009, copies of all significant FOIA requests had to be forwarded to Secretary Napolitano's political staff for review. The career staff in the FOIA office weren't permitted to release responses to these requests without approval from political staff.

Second, career FOIA professionals were burdened by an intrusive political staff and blamed for delays, mistakes, and inefficiencies for which the Secretary's political staff was responsible. The Chief Privacy Officer, herself a political appointee, did not adequately support and defend career staff. To the contrary, in one of her emails, she referred to her career staff as "idiots."

Third, political appointees displayed hostility toward the career staff. In one email, political staff referred to a senior career FOIA employee as a "lunatic" and wrote of attending a FOIA training session organized by the career staffer for the "comic relief." Moreover, three of the four career staff interviewed by the committee have been transferred, demoted, or relieved of certain responsibilities.

Finally, the report finds that the Secretary's office and the General Counsel's office can still withhold and delay significant responses. Although the FOIA office no longer needs an affirmative statement of approval, the Secretary's political staff retains the ability to halt the release of FOIA responses.

The conduct of the political appointees at Homeland Security involved the politically motivated withholding of information about the very conduct of our government from our citizens. In particular, it was the withholding of information about the administration's controversial policies and about its mistakes. This was a direct violation of the President's orders.

I'm disappointed that there wasn't more coverage of Chairman Issa's report and the inappropriate conduct by political appointees at Homeland Security. I'm also disappointed that the Justice Department hasn't conducted an investigation of this scandal.

I have to say that I'm a bit surprised that some open government and privacy groups appear to be accepting the dramatic regulatory power that Homeland Security and Secretary Napolitano will have under the Lieberman-Collins' cybersecurity bill and under President Obama's proposal. Given the FOIA scandal at Homeland Security, I'd have thought that they'd have more reservations.

I'm also sorry to say that the Department of Homeland Security isn't alone when it comes to questionable actions. Recently, the National Security Archive gave its annual Rosemary Award to the Department of Justice for the worst open government performance in 2011.

The charges the Archive makes against the Justice Department include:

(1) proposing regulations that would allow the government to lie about the existence of records sought by FOIA requesters, and that would further limit requestors ability to obtain information;
(2) using recycled legal arguments for greater secrecy, including questionable arguments before the Supreme Court in 2011 in direct contradiction to President Obama's presumption of openness; and
(3) backsliding on the key indicator of the most discretionary FOIA exemption, Exemption 5 for deliberative process. In 2011, the Justice Department cited Exemption 5 to withhold information 1,500 times. That's up from 1,231 times in 2010.

According to the Archive, the Justice Department edged out a crowded field of contending agencies that seem to be in "practical rebellion" against President Obama's open-government orders.

So there's a disturbing contradiction between President Obama's grand pronouncements and the actions of his political appointees. The Obama administration doesn't understand that open government and transparency must be about more than just pleasant sounding words in memos. Ultimately, the President is responsible for the conduct of his political appointees, especially after three years in office. Both he and Attorney General Holder certainly know what's been going on.

Throughout my career I've actively conducted oversight of the Executive Branch regardless of who controls the Congress or the White House.

Open government isn't a Republican or a Democrat issue. It has to be a bipartisan issue. It's about basic good government and accountability—not party politics or ideology.

I started out my remarks by quoting James Madison, the Founding Father who is one of the inspirations for Sunshine Week. Madison understood the danger posed by the type of conduct we're seeing from President Obama's political appointees. He explained that --- "[a] popular government without popular information or the means of acquiring it, is but a prologue to a farce, or a tragedy, or perhaps both."

So I'm looking forward to hearing the testimony of the witnesses. Their experiences and expertise should be helpful. I want to thank all of the witnesses for coming in and for taking the time to prepare their testimony.

I also want to thank Sargent Ensminger for his service to our country. I'm very sorry about the loss of your daughter. I'm a cosponsor of the Caring for Camp Lejeune Veterans Act, which was introduced by Senator Burr. That bill will help to provide medical treatment and care for service members and their families, who lived at the camp and were injured by the chemical contamination.

Thank you.

-30-

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Committee On The Judiciary,
Hearing On "The Freedom Of Information Act: Safeguarding
Critical Infrastructure Information And The Public's Right To Know"
March 13, 2012

Today, the Committee holds an important hearing on one of our most cherished open government laws, the Freedom of Information Act (FOIA). We also commemorate Sunshine Week – an annual celebration of transparency in our democratic society – which is being celebrated across the Nation this week.

In the decade since September 11, Congress has wrestled with how best to maintain the careful balance between Government secrecy and the public's right to know as new threats to national security emerge. Of course, Government secrecy has its place. But, Government officials will always be tempted to overuse the secrecy stamp. And when that happens, *excessive* Government secrecy can come at an unacceptable price – harm to the American public's interests in safety, healthy living and a clean environment.

Sunshine Week is a timely reminder that, as the Congress considers how best to safeguard critical infrastructure information in cyberspace, we must also safeguard the American public's right to know about threats to their health and safety. Last year, the Supreme Court held in *Milner v. Navy* that the Government could not rely upon exemption 2 under FOIA to withhold explosives maps from the public. The *Milner* decision was an important victory for open government. But, in its wake, Congress is considering several new legislative exemptions to FOIA for critical infrastructure information. We should do so carefully.

In January, President Obama signed into law a carefully-balanced, narrow exemption to FOIA for Department of Defense critical infrastructure information. I helped craft this provision as part of the National Defense Authorization Act (NDAA). That measure requires Government officials to affirmatively determine that withholding critical infrastructure information from the public outweighs other interests – such as ensuring that citizens have access to health and safety information. This measure will allow the Government to safeguard truly sensitive information, while also safeguarding the public's right to know about health and safety dangers.

As Congress considers other proposed legislative exemptions to FOIA for critical infrastructure information, I intend to work with Members on both sides of the aisle to ensure that the public's interest in accessing essential health and safety information is protected.

President Obama has made an historic commitment to restoring the presumption of openness to our Government. I commend the Obama administration for taking many important steps to improve transparency, such as the "ethics.gov portal" that the administration launched last week to provide greater public access to ethics and campaign finance reports. But, more progress is needed to fulfill the commitment to open government that I share with the President.

I am pleased that representatives from the Department of Justice and the National Archives and Records Administration are here to discuss how the Obama administration is handling critical infrastructure information under FOIA in the wake of the *Milner* decision. We also have a distinguished panel of expert witnesses.

Securing our Nation's critical infrastructure information is without question a pressing national priority. But, unless we also safeguard the public's right to know about threats to health and safety, the American people will be kept in the dark about dangers that directly affect their lives. This Committee has long recognized that ensuring the public's right to know is neither a Democratic nor a Republican issue, but an issue of importance to all Americans. I hope that this bipartisan tradition will continue as the Congress considers new exemptions to the Freedom of Information Act for critical infrastructure information.

# # # #

The New York Times

The Power to Kill

March 10, 2012

President Obama, who came to office promising transparency and adherence to the rule of law, has become the first president to claim the legal authority to order an American citizen killed without judicial involvement, real oversight or public accountability.

That, regrettably, was the most lasting impression from a major address on national security delivered last week by Attorney General Eric Holder Jr.

There were parts of the speech worth celebrating — starting with Mr. Holder's powerful discussion of why trying most terrorists in civilian courts is best for punishing them and safeguarding America. But we are deeply concerned about his rejection of oversight and accountability when it comes to killing American citizens who are suspected of plotting terrorist acts.

A president has the right to order lethal force against conventional enemies during conventional war, or against unconventional enemies in unconventional wars. But when it comes to American citizens, there must be compelling evidence that the threat the citizen poses is imminent and that capturing the citizen is not a realistic option.

The case that has brought the issue to international attention is the Sept. 30, 2011, drone strike in Yemen that killed Anwar al-Awlaki, an American citizen, who United States officials say was part of Al Qaeda's command structure. Another American was killed in the strike, and Mr. Awlaki's 16-year-old son, also an American citizen, was killed in an attack two weeks later.

The killings touched off a storm of criticism. Mr. Awlaki's father tried to sue the government, which used the "national secrets" defense to have the case tossed out. But the administration has refused to acknowledge that the killing took place or that there is in fact a policy about "targeted killings" of Americans.

It has even refused to acknowledge the existence of a Justice Department memo providing legal justification for killing American citizens, even though that memo has been reported by The Times and others. It is beyond credibility that Mr. Obama ordered the Awlaki killing without getting an opinion from the department's Office of Legal Counsel. Even President George W. Bush took the trouble to have lawyers in that office cook up a memo justifying torture.

The administration intended Mr. Holder's speech to address the criticism and provide a legal argument for the policy, but it was deeply inadequate in important ways.

Mr. Holder agreed that killing an American citizen requires that he "poses an imminent threat of violent attack against the United States," that capture "is not feasible," that the target has military value, that other people are not targeted intentionally, that the potential "collateral damage" not be excessive and that the weapons used "will not inflict unnecessary suffering."

But he gave no inkling what the evidence was in the Awlaki case, and the administration did not provide a way in which anyone other than the people who gave the order could review whether the standards were met. Mr. Awlaki made tapes for Islamist Web sites that justified armed attacks on the United States by Muslims. But was he just spouting off, or actively plotting or supporting attacks?

All Mr. Holder did say was that the president could order such a killing without any judicial review and that any such operation would have "robust" Congressional oversight because the administration would brief Congressional leaders. He also said the administration provided Congress with the legal underpinnings for such killings.

In the Awlaki case, we do not know whether that notification was done in advance or after the fact, if it was done at all. We do know the administration has not given Congress the legal memo with the underlying justification for killing American citizens, because Senator Patrick Leahy, chairman of the Judiciary Committee, was asking Mr. Holder for it just the other day.

Perhaps most disturbing, Mr. Holder utterly rejected any judicial supervision of a targeted killing.

We have said that a decision to kill an American citizen should have judicial review, perhaps by a special court like the Foreign Intelligence Surveillance Court, which authorizes eavesdropping on Americans' communications.

Mr. Holder said that could slow a strike on a terrorist. But the FISA court works with great speed and rarely rejects a warrant request, partly because the executive branch knows the rules and does not present frivolous or badly argued cases. In Mr. Awlaki's case, the administration had long been complaining about him and tracking him. It made an earlier attempt to kill him.

Mr. Holder said such operations require high levels of secrecy. That is obvious, but the FISA court operates in secret, and at least Americans are assured that some legal authority not beholden to a particular president or political party is reviewing such operations.

Mr. Holder argued in his speech that judicial process and due process guaranteed by the Constitution "are not one and the same." This is a straw man. The judiciary has the power to say what the Constitution means and make sure the elected branches apply it properly. The executive acting in secret as the police, prosecutor, jury, judge and executioner is the antithesis of due process.

The administration should seek a court's approval before killing an American citizen, except in the sort of "hot pursuit" that justifies the police shooting of an ordinary suspect. There should be consequences in the event of errors — which are, tragically, made, and are the great risk. And

the administration should publish the Office of Legal Counsel memo. We cannot image why Mr. Obama would want to follow the horrible example set by Mr. Bush in withholding such vital information from the public.

TESTIMONY OF MIRIAM NISBET

DIRECTOR OF THE OFFICE OF GOVERNMENT INFORMATION SERVICES

BEFORE THE SENATE COMMITTEE ON THE JUDICIARY

ON

"THE FREEDOM OF INFORMATION ACT: SAFEGUARDING CRITICAL INFRASTRUCTURE AND THE PUBLIC'S RIGHT TO KNOW"

MARCH 13, 2012

Good morning, Mr. Chairman, Senator Grassley, and members of the committee. I am Miriam Nisbet, Director of the Office of Government Information Services at the National Archives and Records Administration. Thank you for the opportunity to appear before you during Sunshine Week to discuss safeguarding critical infrastructure information. An important part of the Freedom of Information Act is protecting sensitive information even as the government strives to give the public the greatest access to records under the law.

I hope to provide you with a sense of what we are hearing from requesters and agencies with regard to safeguarding critical infrastructure information and other records previously protected under Exemption 2 to the FOIA. In our work at OGIS, we talk every day with agency FOIA professionals and FOIA requesters — in fact, we have worked with requesters and agencies on more than 1,500 specific FOIA matters since we opened in September 2009. Congress created OGIS as part of the 2007 amendments to FOIA to review agency FOIA policies, procedures and compliance; to recommend policy changes to Congress and the President to improve the administration of FOIA; and to resolve FOIA disputes between agencies and requesters. Carrying out this mission allows us to see how agencies implement the

law and shows us where there are trouble spots. We regularly meet with and hear from requesters and agency professionals to discuss trends, problems, complaints and improvements to FOIA's implementation. And the dispute-resolution skills training that we provide to hundreds of agency FOIA professionals each year allows us to hear their questions and concerns.

FOIA law changed significantly with the decision by the Supreme Court of the United States in *Milner v. Department of the Navy*.[1] Although it has been one year since *Milner* was decided, its impact still feels very fresh. As you know, the *Milner* decision addressed the Navy's use of Exemption 2 in withholding maps and data from the Naval Magazine Indian Island base in Washington State. [Note: NARA's understanding is that the basics of the Court's decision will be addressed in DOJ's testimony, therefore NARA oral testimony will refer to the DOJ explanation and will not go into the following details.] Exemption 2 shields records "related solely to the internal personnel rules and practices of an agency."[2] For 30 years, the U.S. Court of Appeals for the D.C. Circuit read Exemption 2 to cover two separate broad categories of information :[3] "High 2" would cover any "predominantly internal materials" the disclosure of which would "significantly ris[k] circumvention of agency regulations or statutes,"[4] and "Low 2" would apply to records concerning human resource and employee relations. The Supreme Court in *Milner* rejected this interpretation last year, holding that only the narrower "Low 2" reading of Exemption 2 was proper: "Exemption 2 … encompasses only records relating to issues of employee relations and human resources,"[5] the Court wrote. Although the records at issue in that case were acknowledged by the Court to be sensitive and of potential use to those wishing to

[1] 562 U.S. _____ (2011); 131 S.Ct. 1259 (2011).
[2] 5 U.S.C. § 552(b)(2).
[3] *Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 670 F.2d 1051 (1981).
[4] *Id.* at 1056-57 and 1074.
[5] *Milner*, 131 S.Ct. at 1271.

cause harm, the Court held: "The explosives maps and data requested here do not qualify for withholding under that exemption."[6]

The net practical effect of *Milner* alongside the DOJ guidance issued in its wake[7] is that Exemption 2 can no longer be used to protect an entire category of internal government information not related to employee relations and human resources — including the critical infrastructure information that is the focus of today's hearing. Following the *Milner* decision, OGIS heard concerns from both agencies and requesters about potential repercussions to FOIA implementation. Agencies were trying to determine how to treat information previously covered by Exemption 2. Two paths were fairly clear from the Supreme Court's decision and from subsequent written guidance from DOJ: if release would not likely result in foreseeable harm to an identifiable interest, the information should be released; and if release would be harmful and another exemption could apply, the information could be withheld under that exemption.

Existing exemptions are a solution for some information that may have previously been withheld under Exemption 2, and OGIS is hearing from agencies that they have taken the Supreme Court's suggestion and used the DOJ's guidance to identify the types of records that might be protected under other exemptions. However, other exemptions are not an alternative for many records in many instances. For example, Justice Alito's concurring opinion in *Milner* focused on the potential application of Exemption 7[8] to withhold information related to crime prevention and security.[9] Of course, Exemption 7 is available only for "records or information compiled for law enforcement purposes." For many agencies, Exemption 7 is off the table

---

[6] *Id.*

[7] Department of Justice Office of Information Policy Guidance titled "Exemption 2 After the Supreme Court's Decision in *Milner v. Department of the Navy*" (May 10, 2011).

[8] 5 U.S.C. § 552(b)(7).

[9] *See Milner*, 131 S.Ct. at 1272.

entirely. Similarly, Exemption 1,[10] which protects properly classified national security information, is also limited in its use. Not only is expanding the amount of classified information undesirable as a matter of policy and practicality; not all agencies have classification authority.

And for that information that falls into a third category — where release would be harmful but no other exemption could apply — agencies were left without a clear cut way to protect sensitive information that had been protected from release for decades. In such cases, records such as risk and vulnerability assessments to physical or electronic systems, unclassified details regarding military operations; and sensitive, operational information (such as computer codes, telecommunication passcodes and certain information contained in staff manuals) would appear to be without protection from release as well.

Requesters as well as agencies have indicated to us the need for changes to FOIA post-*Milner*. Acknowledging that some legislative action is warranted, requesters worry this may come in the form of multiple federal laws containing provisions to allow information to be withheld from release under FOIA Exemption 3.[11] "Exemption 3 statutes" provide a solution for only the limited subject matter at issue, typically contained in a more comprehensive piece of legislation, which means dozens of such statutes, would potentially be required to cover the various agency-specific information currently unaddressed by existing FOIA exemptions.

Additionally, as this Committee has observed, Exemption 3 statutes can be difficult to track as they move through the legislative process. Requesters are concerned that they may not be able to monitor the progress of these many disparate laws either as they are proposed or as they are used by agencies subsequent to enactment. Finally — a concern for both agencies and requesters —an ad hoc approach of passing Exemption 3 statutes could result in the uneven

[10] 5 U.S.C. § 552(b)(1).
[11] 5 U.S.C. § 552(b)(3).

application of FOIA disclosure provisions throughout the Federal Government. Even though the Critical Infrastructure Information Act of 2002 defines critical infrastructure information, each agency might define critical infrastructure differently, depending on its mission, and could have its own scheme for how its non-disclosure statute would be implemented.

An alternative and more comprehensive solution suggested by various agencies and FOIA requesters might be to modify the existing Exemption 2 provision. Reworking Exemption 2 to address certain types of information previously protected by "High 2" would help to close the gap left after *Milner* for this critical infrastructure information. This effort could focus on finding a generic approach available across government that takes into account both the concerns of agencies and requestors to address a subset of sensitive information.

We appreciate the Committee's efforts to examine solutions to protect critical infrastructure and other sensitive information that should not be disclosed but in a way that otherwise promotes disclosure consistent with FOIA and with President Obama's 2009 memorandum on FOIA.[12] OGIS stands ready to assist in any way, including working with DOJ to facilitate collaboration between internal and external stakeholders. Thank you for the opportunity to testify; I look forward to answering any questions you may have.

[12] Memorandum from President Barack Obama to the heads of Executive Departments and Agencies titled "Freedom of Information Act" (Jan. 21, 2009)

OFFICE *of* GOVERNMENT INFORMATION SERVICES

April 13, 2012

NATIONAL
ARCHIVES
and RECORDS
ADMINISTRATION

8601 ADELPHI ROAD
COLLEGE PARK, MD
20740-6001

web: www.ogis.archives.gov
e-mail: ogis@nara.gov
phone: 202-741-5770
toll-free: 1-877-684-6448
fax: 202-741-5769

The Honorable Patrick J. Leahy
Chairman
The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley:

This letter responds to your questions during the Committee's recent hearing on the Freedom of Information Act (FOIA) on March 13, 2012. I was pleased to appear before the Committee as the first Director of the Office of Government Information Services (OGIS), created to be the FOIA Ombudsman by the OPEN Government Act of 2007.

In OGIS's first two years, the Office handled more than 1200 requests for assistance, involving 42 agencies and requesters from 48 states, the District of Columbia, several territories and 13 foreign countries. A report on OGIS's first year was made available to the public during Sunshine Week 2011, and its second report was published recently. https://ogis.archives.gov/about-ogis/ogis-reports.htm

These reports, as well as information made available regularly through OGIS's web site, provide details about the kinds of requests for assistance and the types of issues the office is handling, and the outreach and review efforts of the office staff. Both reports highlight agency Best Practices in implementing FOIA and OGIS's expansion of its dispute resolution skills training for FOIA professionals.

As part of OGIS's work towards improving FOIA administration, I appreciated the Committee's questions at the hearing that focused on OGIS's partnership through its parent agency, the National Archives and Records Administration, with the Environmental Protection Agency and the Department of Commerce to collaborate in developing a FOIA portal. We believe that the project has potential to improve the public's access to government information and to save the taxpayers money by sharing agency resources and repurposing existing technology.

During the hearing, you asked about the status of policy recommendations to Congress. OGIS's statutory mission includes "recommend[ing] policy changes to Congress and the President to improve the administration of" FOIA. When OGIS submitted our recommendations to the Office of Management and Budget, we did not recommend any substantive revisions to the disclosure requirements of FOIA. Instead, based on our first year of operations, OGIS's identified recommendations focused on two areas: (1) minimizing misdirected inquiries by members of the public seeking assistance on matters outside OGIS's mandate; and (2) facilitating other agencies' sharing of information with OGIS, consistent with those agencies' legal obligations. OGIS submitted these recommendations to OMB last year, and as a result of the interagency consultation process, OGIS and OMB agreed that progress on these issues could be made administratively.

As noted above, we have thus far focused on improving internal coordination of government operations – and have not proposed any revisions to the disclosure requirements of FOIA. Given this, we do not feel that activities needed to address OGIS's concerns rise to the level of recommendations to Congress at this time. We are pursuing solutions with other agencies before further considering whether a legislative proposal would be necessary or appropriate. I expect to be working with the Privacy Officers Committee of the Chief Information Officers Council on the issues described above, and I would be pleased to update you on my progress in enhancing OGIS's performance of its statutory mission.

Thank you for your continued support of OGIS. We stand ready to answer any questions you may have.

Sincerely,

MIRIAM NISBET
Director, Office of Government Information Services

Cc:

The Honorable Jeffrey Zients
Acting Director
Office of Management and Budget
Washington, DC 20503

The Honorable David S. Ferriero
Archivist of the United States
National Archives and Records Administration
Washington, DC 20408

OFFICE *of* GOVERNMENT INFORMATION SERVICES

NATIONAL
ARCHIVES
and RECORDS
ADMINISTRATION

8601 ADELPHI ROAD
COLLEGE PARK, MD
20740-6001

web: www.ogis.archives.gov
e-mail: ogis@nara.gov
phone: 202-741-5770
toll-free: 1-877-684-6448
fax: 202-741-5769

April 24, 2012

The Honorable Patrick J. Leahy
Chairman
The Honorable Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Leahy and Ranking Member Grassley,

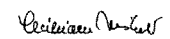
Thank you for your continuing interest in improving the administration of the Freedom of Information Act (FOIA). Enclosed please find a report that describes, in accordance with Title 5 of United States Code, Section 552 (h)(2)(C), policy recommendations and other matters that the National Archives and Record Administration's (NARA) Office of Government Information Services' (OGIS) has identified that could be addressed make further improvements in the administration of FOIA. To provide you with additional background regarding OGIS, which as you know, opened in September 2009, I also have enclosed a report of OGIS' second year of operations, through Fiscal Year 2011. This report provides a description of the types of requests and issues that OGIS has handled. An identical letter and report have been sent to the House Committee on Oversight and Government Reform.

This report, as well as the report on our first year, highlights agency Best Practices and other strategies for making FOIA work better. OGIS also regularly posts on its blog suggestions to improve the FOIA process administratively, such as recently during Sunshine Week: training for all government employees in the basics of FOIA; standardizing agency FOIA web pages, including developing, with stakeholder input, an easy-to-use design template for agencies to customize; top-down agency support for FOIA; and professionalizing the agency FOIA career track.

We appreciate your continued support as OGIS has been transformed from statutory language to reality. Our office is an important symbol of Congress's vision of a better FOIA.

I hope that you find this information helpful as you examine agencies' implementation of FOIA. If you have any further questions, please do not hesitate to call NARA's Office of Congressional Affairs at 202-357-5100.

Sincerely,



Miriam Nisbet, Director
Office of Government Information Services

Enclosures:

OGIS Policy Recommendations for Improving Freedom of Information Act Procedures and the Administration of the Office of Government Information Services, April 2012
OGIS Report: Building A Bridge, March 2012, https://ogis.archives.gov/about-ogis/ogis-reports.htm

cc:
The Honorable Joseph I. Lieberman, Chairman, United States Senate, Committee on Homeland Security and Governmental Affairs
The Honorable Susan Collins, Ranking Member, United States Senate, Committee on Homeland Security and Governmental Affairs

OGIS Policy Recommendations for Improving Freedom of Information Act procedures and the Administration of the Office of Government Information Services

April 24, 2012

The National Archives and Records Administration's (NARA) Office of Government Information Services (OGIS) has identified a number of areas where the Freedom of Information Act (FOIA) process could be improved, as well as areas where OGIS's role can be made more effective. The policy recommendations, prepared in accordance with Title 5 of United States Code, Section 552 (h)(2)(C), have benefitted from ongoing consultation with agencies as well as feedback from the public.[1] OGIS is currently working to implement these recommendations, and looks forward to engaging with Congress in these areas.

Issue 1: Misdirected Inquiries from the Public

Challenge:
OGIS regularly receives calls from members of the public looking for assistance with requests for their own records, although OGIS's statutory authority does not include such first-party requests under the Privacy Act of 1974. These requesters are often uncertain about the application of FOIA and the Privacy Act when agencies process requests for access to records. OGIS initially saw its role as limited to assisting only with straight FOIA requests. Over time, OGIS realized that many first-party, or Privacy Act, requests overlap with the FOIA. OGIS works to provide ombuds services for such requests, including providing information about the process and the status of requests. OGIS also acts to ensure that the administrative process is fair. OGIS does not have a statutory role in reviewing policies, procedures and compliance with the Privacy Act as it does with FOIA. Although not a large part of the OGIS caseload, providing ombuds services to Privacy Act requesters does compete with the Office's implementing fully its mission of assisting FOIA requesters. In addition, OGIS has observed that the level of service and assistance to first-party requesters can be improved.

Recommendation and Action Step:
The Chief Information Officers Council has taken steps to make it easier for individuals to find the Department and Agency Privacy homepages, http://www.cio.gov/modules/privacy/. Because of the intersection of FOIA and the Privacy Act, OGIS, working with the Privacy Officers Committee of the CIO Council, should help to develop and promote methods for departments and agencies, which receive large volumes of first-party requests, to improve how requesters navigate agency processes to obtain needed information.

Issue 2: Facilitating Agencies' Sharing of Information with OGIS

Challenge:
When a FOIA requester initiates contact with OGIS, the Office obtains the requester's signed consent under the Privacy Act of 1974 before assisting him or her. The consent authorizes OGIS to inquire on a customer's behalf regarding the request or administrative appeal at issue; the consent also authorizes

[1] OGIS had previously provided a draft report, prepared in accordance with Title 5 of United States Code, Section 552 (h)(2)(C), to the Office of Management and Budget. The coverage of that draft report was limited to policy issues 1 and 2 described herein.

departments and agencies to release to OGIS information and records related to the request or appeal. However, requiring consent can be an obstacle when an agency, rather than an individual requester, is seeking OGIS assistance. The situation places agencies in the position of obtaining requester consent for the sole purpose of seeking OGIS' assistance in resolving a dispute. (A secondary challenge is that asking for and obtaining the consent adds to the time it takes OGIS to handle a request for assistance.)

Recommendation and Action Step:
OGIS will work with the Office of Management and Budget, which is statutorily charged with implementing government-wide Privacy Act guidance, on language that agencies could use as a model to publish as a Privacy Act (b)(3) routine use in their FOIA requests/appeals Systems of Records Notices. Under consideration is the following language, which will be proposed imminently by the Department of Justice for its FOIA/PA request/appeals files system notice:

"To the National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. 552(h), to review administrative agency policies, procedures, and compliance with the Freedom of Information Act, and to facilitate OGIS' offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies."

Issue 3: Improving Public Access to FOIA Information

Challenge:
About 350 Federal departments, agencies and components comprise the Federal executive branch, and each has its own separate process for accepting and processing FOIA requests; the landscape is complex and some requesters, who have the statutory right under FOIA to seek access to documents, find the bureaucracy difficult to navigate. On the agency side, many FOIA professionals are challenged with processing requests in accordance with the statute, particularly shepherding an abundance of requests through the process and making public frequently requested documents.

Recommendation and Action Step:
OGIS is a partner with the Environmental Protection Agency and the Department of Commerce to collaborate in developing a pilot portal, now called the FOIA Module – a one-stop portal that could be used to accept FOIA requests, store them in a repository for processing by agency staff, and allow responsive documents to be uploaded into the system and posted for the public. The Module is scheduled to be launched for agencies this summer and unveiled to the public in October 2012. OGIS believes that the project has potential to improve the public's access to government information and to save taxpayers' money by sharing agency resources and repurposing existing technology. Based on the results of the launch, OGIS would work with other agencies to consider how the Module might be useful to them in carrying out their statutory responsibilities.

Issue 4: Coordinating FOIA Responses Across Government

Challenge:
It is not uncommon for multiple agencies to receive related, or even identical, FOIA requests. Agency professionals responding to these requests may not be aware of the similar requests, and

may not be taking full advantage of appropriate opportunities to coordinate their efforts in responding.

Recommendation and Action Step:
OGIS developed a strategy to coordinate agency contacts and facilitate communication on multi-agency requests. This approach ensures agencies are aware that the request has been received by fellow agencies; puts the agency points of contact in touch with one another so they can share tips and strategies for fulfilling the request; and also helps to avoid redundancies.

OGIS facilitates discussions via email, telephone and in-person meetings to coordinate communication in which agencies discuss their steps in resolving the requests and raise any concerns or difficulties they have encountered. (OGIS also coordinates with DOJ's Office of Information Policy as appropriate, in view of the offices' complementary roles.) While agencies work autonomously to respond to requests, they can share information with one another to assist in preventing and avoiding disputes and to provide good customer service to requesters. It also allows for discussion of any disparate responses and an opportunity to help requesters understand why agencies may treat similar information in different ways.

OGIS serves as the central point of contact for the agencies in sharing information and also relays information to requesters as appropriate. Both agencies and requesters have found this approach to be very useful and both now initiate requests for OGIS assistance. We believe that this type of coordination reduces the burden on each agency, improves the quality of the response, and provides better service to requesters.

Issue 5: Developing Dispute Resolution Skills in Agency FOIA Professionals

Challenge:
The amended Freedom of Information Act, 5 U.S.C. §§ 552(a)(6)(B)(ii) and (l), now directs FOIA Public Liaisons to help resolve FOIA disputes. However, there has been no comprehensive training effort to help agency FOIA personnel develop dispute resolution skills.

Recommendation and Action Step:
OGIS offers a free dispute resolution skills training program for all FOIA professionals to help them achieve this mandate. We present an inter-agency version of this training program quarterly in collaboration with the Department of Justice's Office of Information Policy (OIP). OGIS also offers agency-specific FOIA dispute resolution skills training; so far we have delivered that training to the FOIA staffs of the Departments of the Interior, State, and Homeland Security. OGIS will encourage departments and agencies to partner with OGIS to expand dispute resolution training for their FOIA professionals. OGIS also intends to develop cross-training for agency Dispute Resolution professionals so that they can assist their FOIA colleagues in preventing and resolving FOIA disputes.

Department of Justice

STATEMENT OF

MELANIE ANN PUSTAY
DIRECTOR
OFFICE OF INFORMATION POLICY

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

PRESENTED

MARCH 13, 2012

Testimony of Melanie Ann Pustay,

Director of the Office of Information Policy

United States Department of Justice

Good morning Chairman Leahy, Ranking Member Grassley, and Members of the Committee. I am pleased to be here during Sunshine Week, to address the effect of the Supreme Court's recent decision in *Milner v. Department of the Navy* on agencies' administration of the Freedom of Information Act (FOIA) and to discuss the Department of Justice's continued efforts of the past year to ensure that President Obama's January 21, 2009 Memorandum on the FOIA, as well as Attorney General Holder's FOIA Guidelines, are fully implemented. As the lead federal agency responsible for implementing the FOIA across the government, the Department of Justice is strongly committed to encouraging compliance with the Act by all agencies and to promoting open government.

The Attorney General issued his new FOIA Guidelines during Sunshine Week three years ago, on March 19, 2009. The Guidelines address the presumption of openness that the President called for in his FOIA Memorandum, the necessity for agencies to create and maintain an effective system for responding to requests, and the need for agencies to proactively and promptly make information available to the public. Stressing the critical role played by agency Chief FOIA Officers in improving FOIA performance, the Attorney General called on all Chief FOIA Officers to review their agencies' FOIA administration each year and to report to the Department of Justice on the steps taken to achieve improved transparency. These Chief FOIA

Officer Reports were completed last week for the third time since the Attorney General's FOIA Guidelines were issued.

The Chief FOIA Officer Reports have become an invaluable tool for assessing agency implementation of the FOIA Guidelines. Each year they have also illustrated the broad array of activities agencies have undertaken to improve their administration of the FOIA and to improve transparency overall. This past year, the Department of Justice directed agencies to address new questions in their Chief FOIA Officer Reports that build on the successes of the 2011 Reports. For example, in addition to asking agencies to describe their efforts to make information available on agency websites, for 2012, we asked agencies to also address any steps that had been taken to make that posted information more useful to the public. Based on our review of both the Chief FOIA Officer Reports and agency Annual FOIA Reports, it is clear that agencies continue to make real progress in applying the presumption of openness, improving the efficiency of their FOIA processes, reducing their backlogs of pending FOIA requests, expanding their use of technology, and making more information available proactively. While there is always more work to be done, for the third year in a row, agencies have shown that they are improving FOIA compliance and increasing transparency.

In Fiscal Year 2011, agencies were faced with an increase in the number of incoming FOIA requests, which rose from 597,415 in Fiscal Year 2010 to 644,165 in Fiscal Year 2011. Notably, the Department of Homeland Security experienced a 35% increase in the number of incoming requests. Overall, agencies were able to increase the number of requests that they processed in Fiscal Year 2011, increasing the number of processed requests by 30,575. Most significantly, when agencies processed those requests they increased the amount of material that

was provided to the requester. Indeed, for those requests where records were located and processed for disclosure, the government released records in full or in part for 93.1 % of those requests. This marks the third straight year in which the government achieved such a high release rate. This sustained, high release rate is a tribute to the efforts of FOIA professionals across the government as they work tirelessly to apply the FOIA Guidelines to the hundreds of thousands of requests they process throughout the year.

Agencies also continue to meet the demand for public information by proactively posting information of interest to the public. For example, the Department of Education annually receives more than 700 requests for contracts, grant applications, and information about federally funded programs. Through efforts to proactively identify these records and post them online, the Department of Education increased the amount of material it proactively disclosed in its FOIA Library by 25%. The Department of Homeland Security increased the amount of information it proactively released by 43%, posting nearly nine thousand pages of new information on its website. Similarly, the Department of State added over two thousand documents to its online Rwandan Declassification Collection. Within a day of issuing the long-awaited accident report for the 2010 Upper Big Branch mining disaster, the Department of Labor's Mine Safety and Health Administration posted a substantial amount of supporting data that was considered in the report, including nearly 30,000 pages of interview transcripts.

In addition to proactively posting new information, many agencies have also taken steps to make the information on their websites more useful to the public. Several agencies undertook efforts this past year to redesign their websites to make them more user-friendly and to improve their websites' search capabilities. For example, the Department of Energy recently consolidated

and upgraded several websites into a new department-wide website, which utilizes interactive maps and graphics to display information in a more accessible format and allows users to search for documents and resources using a single search engine. Agencies are utilizing online portals and dashboards to facilitate access to information. For example, the Department of Energy created a FOIA portal that is full-text searchable and provides access to documents previously released under the FOIA. The Department of Agriculture added material to its Tribal Institutions Portal to provide information on applying for and managing grants. The Federal Aviation Administration launched a new online dashboard to provide the public with information on the modernization of air transportation system infrastructure. The Department of Transportation is publishing information through an Application Program Interface. Numerous components of the Department of Defense made improvements to their websites, created systems to facilitate the proactive posting of contracts, and used social media to educate the public in real time about vital information on available programs and resources, such as those relating to traumatic brain injury. The Department of Health and Human Services' Administration for Children and Families has installed a live chat feature on the website of its Child Welfare Information Gateway, through which users can engage with an Information Specialist who will assist with questions, concerns, or trouble locating information.

Embracing the President's FOIA Memorandum and the Attorney General's Guidelines, many agencies have gone beyond using their websites to disseminate information of public interest and have increasingly utilized social media tools such as blogs, Twitter, Facebook, and YouTube to reach a wider audience. For example, the Internal Revenue Service posted Tax Tips videos on YouTube in English, Spanish and sign language, and is in the process of promoting a

smartphone application called IRS2Go, which will give users a convenient way of checking their federal refund status and obtaining easy-to-understand tax tips. The U.S. Customs and Border Protection continued using YouTube videos, Twitter and Flickr this past year to proactively release information about seizures and other activities related to its mission. Similarly, the Department of Education notified the public of important events and provided information through its blog, electronic newsletters, Twitter, Facebook, and YouTube. These are just a few of the many examples of notable agency accomplishments that are detailed in the agency Chief FOIA Officer Reports for 2012.

I am also pleased to report that this past fiscal year many agencies were able to reduce their FOIA backlogs. Ten of the fifteen cabinet agencies reduced their backlog of pending requests for Fiscal Year 2011. For example, despite receiving over 3,500 more requests this past fiscal year than in Fiscal Year 2010, the Department of Health and Human Services reduced its backlog by 32%. The Department of Defense made a concerted effort this past year to reduce its backlog, with several of its components raising backlog concerns directly with their senior leadership offices. As a result of these efforts, the Defense Logistics Agency, National Geospatial-Intelligence Agency, and Defense Intelligence Agency reduced their backlogs by 69%, 38%, and 29%, respectively, with the agency overall reducing its backlog by 5%. The Department of State was able to achieve an impressive backlog reduction of 60% by streamlining its process for handling the substantial amount of referrals it receives each year. The Department of Interior was also able to reduce its backlog, achieving a 25% reduction.

Despite these significant backlog reduction efforts by many of the large Departments, overall the government had an increase in the FOIA request backlog this past fiscal year. This

increase can be traced to the dramatic increase in the number of FOIA requests received by the Department of Homeland Security, which, in turn, contributed to a much higher request backlog at that agency.

I am particularly pleased to report on the successes achieved by the Department of Justice. This past fiscal year, the Department increased the number of responses to FOIA requests in which records were released in full or in part. Fiscal Year 2011 also marked the second straight year in which the Department maintained a record high 94.5% release rate for requests involving responsive records. Perhaps even more significant, the Department released records in full in response to 79% of requests where records were released. Further, despite three straight years of receiving over 60,000 requests, the Department increased the number of requests processed and reduced our backlog of pending requests by 26%. A parallel reduction in backlog was achieved for pending administrative appeals, with OIP reducing that backlog by a full 41%. The Department also improved the average processing time for both simple and complex FOIA requests. All of these things, both at DOJ and across the government, are concrete examples of improvements made to the administration of the FOIA. There is still work to be done, but we are continuing to make significant, tangible progress in implementing Attorney General Holder's FOIA Guidelines and President Obama's FOIA Memorandum.

My Office carries out the Department's statutory responsibility to encourage compliance with the FOIA. We have been actively engaged from the very start in a variety of initiatives to inform and educate agency personnel on the Administration's commitment to open government and to specifically encourage compliance with both the letter of the law and the spirit of openness that form the foundation for the directives from the President and the Attorney General.

Our engagement started within two days of issuance of the President's FOIA Memorandum, when OIP sent initial guidance to agencies informing them of the significance of the President's Memorandum and advising them to begin applying the presumption of disclosure immediately to all decisions involving the FOIA. OIP issued extensive written guidance which provided agencies with concrete steps to use and approaches to follow in applying the presumption of openness. In the past two years, OIP has provided agencies with additional guidance addressing a range of issues relating to the FOIA. In issuing this guidance, OIP has listened to concerns raised by the FOIA requester community and on multiple occasions has created policy guidance to specifically address those concerns.

I have also reached out to, and met individually with the Chief FOIA Officers of those cabinet agencies that receive and process the overwhelming share of FOIA requests. Additionally, as part of the Department's Open Government Plan, I joined the Associate Attorney General, who is the highest-ranking Chief FOIA Officer in the government, in several meetings with all the Chief FOIA Officers of the cabinet agencies to discuss the implementation of the Attorney General's FOIA Guidelines and other open government initiatives. These meetings have become an invaluable opportunity for the Chief FOIA Officers to hear directly from the Department of Justice as we promote the goals of the President's and the Attorney General's directives and reinforce our joint commitment to openness and transparency.

Since the issuance of the Attorney General's FOIA Guidelines, OIP has also conducted numerous training sessions specifically focused on the President's and Attorney General's transparency initiative. In 2011, OIP conducted forty-seven separate training sessions for agency personnel and also continued to reach out to the public and the requester community. In 2009,

OIP began holding roundtable meetings with interested members of the FOIA requester community to engage in a dialogue and share ideas for improving FOIA administration. In response to the interest expressed by agency FOIA professionals in being able to attend the Requester Roundtables, and the enthusiastic response by the requester community to the idea of meeting with those FOIA professionals, shortly after Sunshine Week last March, OIP held the first-ever FOIA Requester-Agency Town Hall meeting. The Town Hall event was a great success, bringing agency FOIA personnel and frequent FOIA requesters together to exchange ideas, share concerns, and engage in a discussion of common issues. OIP plans to make the FOIA Town Hall an annual event and will be convening the next one in the coming months.

As you know, each year, agencies submit to the Department of Justice their Annual FOIA Reports, which contain detailed statistics on the number of requests and appeals received and processed, their disposition, and the time taken to respond. This past year, OIP updated both its guidance for preparing the Annual Reports and the tool developed by the Department which assists agencies in providing their data in an "open" format as required by the Open Government Directive. The Department continues to receive very positive feedback from agencies on the value of using the tool, with its built-in math checks and other features that alert agencies to data integrity issues. Agency Annual FOIA Reports for Fiscal Year 2011 are posted together on OIP's website and the data from the reports has been added to FOIA.Gov, the Department's new governmentwide, comprehensive FOIA website.

FOIA.Gov has revolutionized the way in which FOIA data is made available to the public. While initially envisioned as a "dashboard" to illustrate statistics collected from agency Annual FOIA Reports, the Department almost immediately began to expand its capabilities and

we continue to add new features each year. With well over a million visitors since it was launched last March, the website has become a valuable resource for both the requester community and agency FOIA personnel. The website takes the detailed statistics contained in agency Annual FOIA Reports and displays them graphically. FOIA.Gov allows users to search and sort the data in any way they want, so that comparisons can be made between agencies and over time.

FOIA.Gov also serves as an educational resource for the public by providing useful information about how the FOIA works, where to make requests, and what to expect through the FOIA process. Explanatory videos are embedded into the site and there is a section addressing frequently asked questions and a glossary of FOIA terms. FOIA contact information is provided for each agency, including their Chief FOIA Officer and all their FOIA Requester Service Centers and FOIA Public Liaisons. Further, the website spotlights significant FOIA releases and gives the public examples of record sets made available by agencies to the public.

In our most recent improvements to the site, we expanded its scope in yet another way by adding a new feature designed to help the public locate information. We added a search tool to FOIA.Gov that allows the public to enter search terms on any topic of interest. FOIA.Gov then searches for information on that topic across all federal government websites at once. This search tool captures not just those records posted in agency FOIA Libraries, but also records posted anywhere on an agency's website. This more expansive search capability is particularly significant given the steady stream of information that agencies are making available proactively on their websites. FOIA.Gov's search tool provides an easy way for a potential FOIA requester to first easily see what information is already available on a topic. This might preclude the need

to even make a request in the first instance, or might allow for a more targeted request to be made.

We launched yet another new feature just a few weeks ago, by including hyperlinks to agency online request forms. As agencies look for ways to improve the FOIA process and to increase efficiency, many have developed the capability to accept FOIA requests online. Currently there are 111 offices throughout the government that provide requesters with the ability to make a request online. As part of the Department's continuing efforts to improve FOIA.Gov, we have added links to these online forms to FOIA.Gov, so that when a requester is on the site and decides to make a request to an agency with online request-making capability, with just "one click" the request can be made directly from FOIA.Gov. I am very pleased to report that OIP itself has just launched an online capability which allows the public to make requests for the leadership offices of the Department online and also to file an administrative appeal online. OIP's online portal allows the public to establish their own user accounts so that they can track the status of their request or appeal at any time online. Requesters will also receive their determinations from OIP via their online accounts, as well as the documents responsive to their requests. As we move forward the Department will look to enhance the OIP Portal to ensure compliance with the President's National Strategy for Trusted Identities in Cyberspace. This policy calls for the development of interoperable digital credentials that reduce the need for users to create multiple account credentials and passwords to access online services. As more and more agencies add this capability to their FOIA programs they will be harnessing the power of technology to improve FOIA processing, in keeping with the President's and

Attorney General's focus on better utilization of technology to make information available to the public.

In addition to our work in implementing the Attorney General's FOIA Guidelines, one of OIP's key responsibilities is developing legal guidance to assist agencies in complying with the many legal requirements of the FOIA. That guidance is particularly needed when there are major changes in the law, such as occurred with the dramatic narrowing of Exemption 2 by the Supreme Court in *Milner v. Department of the Navy,* 131 S. Ct. 1259 (2011).

As you know, in *Milner* the Supreme Court overturned thirty years of established FOIA precedent by restricting the scope of Exemption 2 to matters related solely to *personnel* rules and practices. In doing so, the Court significantly narrowed the reach of Exemption 2, leaving exposed many different types of sensitive information, such as critical infrastructure and cyber security information, or information like that at issue in *Milner* itself, which concerned explosives and weapons data for munitions stored at a Naval facility where the concern was that disclosure would threaten the security of the base and the surrounding community.

Prior to *Milner*, agencies had long followed the expansive interpretation of Exemption 2 provided by the Court of Appeals for the District of Columbia Circuit in *Crooker v. ATF,* 670 F.2d 1051, 1073-74 (1981). In *Crooker*, the D.C. Circuit ruled that Exemption 2 -- which by its terms exempts from mandatory disclosure under the FOIA matters "related solely to the internal personnel rules and practices of an agency" -- should be interpreted more broadly according to a two-part test. Under *Crooker* the information first had to qualify as "predominantly internal" and second, it had to be either of no public interest or trivial in nature, which was referred to as "Low 2," or be more substantial in nature if disclosure would risk circumvention of the law, which was

referred to as "High 2." The D.C. Circuit reasoned that this interpretation of the exemption "flowed from FOIA's 'overall design,' its legislative history, 'and even common sense' because Congress could not have meant to 'enac[t] a statute whose provisions undermined . . . the effectiveness of law enforcement agencies.'" *Milner v. Department of the Navy*, 131 S. Ct. 1259, 1263 (2011) (quoting *Crooker*, 670 F.2d at 1074).

A substantial body of caselaw was developed over the years concerning "High 2," with courts upholding protection for many different types of sensitive information when its disclosure would risk circumvention of the law. Protection was afforded to information such as guidelines for undercover agents, vulnerability assessments, security techniques, audit guidelines, agency testing materials, agency credit card numbers, military rules of engagement, guidelines for protecting government officials, and records pertaining to aviation watch lists and other watch lists and information pertaining to the security of our borders maintained fornational security purposes.

The Supreme Court in *Milner*, however, rejected the *Crooker* court's recognition of "High 2" as inconsistent with the plain language of Exemption 2. Based on the plain language of the exemption, the Supreme Court ruled that the exemption's reach was limited to matters solely related to "personnel." It was the term "personnel," that the Court found "most clearly marks the provision's boundaries." *Id.* at 1264. As a result of that ruling, a wide range of sensitive material whose disclosure could cause harm and which had been protected under the D.C. Circuit's "High 2" formulation of the exemption is now at risk. A legislative amendment to Exemption 2 is critical in order to alleviate that risk.

For three decades, agencies had protected under "High 2" homeland-security and critical

infrastructure information, law enforcement procedures, audit criteria, and other information that, if disclosed, would risk circumvention of the law. Although it limited the scope of Exemption 2 to matters related solely to internal *personnel* rules and practices, the Supreme Court was sympathetic to the policy concerns raised by the government concerning the need to protect information when its disclosure risked harm. The Supreme Court stated that it "recognize[d] the strength" of the Department of the Navy's interest in the case before it to "safely and securely store military ordinance." Indeed, the Court went on to note that "[c]oncerns of this kind—a sense that certain sensitive information *should* be exempt from disclosure—in part led the *Crooker* court to formulate the High 2 standard." *Id.* at 1270-71. The Court acknowledged that it might be necessary for the Government to "seek relief from Congress." *Id.* at 1271.

The Supreme Court suggested that agencies might, in some circumstances, be able to utilize other FOIA exemptions to protect material previously covered by High 2. In OIP's guidance to agencies we suggested just that and provided agencies with possible alternatives to Exemption 2. Nonetheless, it is unlikely that existing FOIA exemptions will suffice to protect, in all instances, every category of information whose release could cause harm.

In the months since the decision in *Milner* some agencies have sought statutory relief from mandatory disclosure under the FOIA for discrete categories of records they maintain. This piecemeal approach, using separate withholding statutes that then fall under Exemption 3 of the FOIA, is not the ideal solution. Such an approach does not sufficiently ensure protection for all agencies and for all categories of information that were long protected under "High 2" and now are at risk of disclosure. The Supreme Court's decision in *Milner* was based on the plain language of Exemption 2. In turn, the Department of Justice believes that the preferred course of

action would be to amend Exemption 2 so that its plain language addresses the need to protect against disclosures that would risk circumvention of the law.

Open Government groups, reporters, and other interested members of the FOIA requester community are understandably interested in this issue as well. The precise contours of a proposed legislative amendment to Exemption 2 will need to take into account both the interests of the agencies in preventing circumvention of the law and safeguarding national security – an interest with which requesters undoubtedly would not disagree – and the shared interests of the requesters and the Department in ensuring that exemptions are precisely crafted so as to not unnecessarily sweep too broadly. Given that agencies and the public have had three decades of experience with a far more robust Exemption 2, one that provided for protection against risk of circumvention of the law, and in light of the fact that there is legislative history supporting such a reading, amending the exemption to reinstate that protection should be informed by that prior experience and history.

In closing, the Department of Justice looks forward to working together with the Committee on all matters pertaining to the government-wide administration of the FOIA, including efforts to protect the vital interests that have been left exposed by the Supreme Court's *Milner* opinion. I would be pleased to address any question that you or any other Member of the Committee might have on this important subject.

STATEMENT

of

Paul Rosenzweig
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Visiting Fellow, The Heritage Foundation
Washington, D.C.

before the

Committee on the Judiciary
United States Senate

March 13, 2012

Cybersecurity Information Sharing and the Freedom of Information Act

Introduction

Chairman Leahy, Ranking Member Grassley, and Members of the Committee, I thank you for your invitation to appear today and present testimony on the question of cybersecurity information sharing and the Freedom of Information Act (FOIA). My name is Paul Rosenzweig and I am the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a Senior Advisor to The Chertoff Group and a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy. In addition, I serve as a Visiting Fellow with a joint appointment in the Center for Legal and Judicial Studies and the Douglas and Sarah Allison Center for Foreign Policy Studies at The Heritage Foundation.[1] From 2005 to 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

[1] The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2010, it had 710,000 individual, foundation, and corporate supporters representing every state in the U.S. Its 2010 income came from the following sources:

Individuals	78%
Foundations	17%
Corporations	5%

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived from prior academic work I have done in this field, most notably a research paper I published under the auspices of the Hoover Institution's Koret-Taube Task Force on National Security and Law, entitled "Cybersecurity and Public Goods: The Public/Private 'Partnership.'"[2] The paper, in turn, will appear as two chapters in my forthcoming book, *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World* (Praeger Press 2012).

In my testimony today, I want to make six basic points:

- The cyber threat is real and likely enduring;
- The sharing of cyber threat and vulnerability information is a classic public good whose creation needs to be enabled by the government;
- Current law is, at best, ambiguous (and at worst prohibitory) and therefore impedes the creation and sharing of cyber threat and vulnerability information;
- The legal régime therefore requires modification to authorize and enable the sharing of vital cyber threat and vulnerability information;
- Essential sharing by the private sector will not occur if ambiguity is maintained or the specter of disclosure is not relieved; and
- Finally, it is therefore essential that a blanket FOIA exemption be part of any new cybersecurity information-sharing legislation.

The Cyber Threat Is Real

On the day I sat down to begin drafting this testimony the NASA Inspector General reported that a significant Chinese penetration of the computer system at the Jet Propulsion Laboratory had occurred.[3] Something on the order of 22 gigabytes of data that contained export-restricted information had been exfiltrated from the computer system of one of the most prominent American laboratories over a period of several months. Sensitive U.S. space information was stolen or destroyed and a laptop with the algorithms to control the International Space Station was also stolen. Only recently had all of this come to light.

The top five corporate givers provided The Heritage Foundation with 2% of its 2010 income. The Heritage Foundation's books are audited annually by the national accounting firm of McGladrey & Pullen. A list of major donors is available from The Heritage Foundation upon request.

Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

[2] http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf

[3] http://quantum.nasa.gov/materials/2012-01-21-A4-Williams.pdf

This is not, of course, the only recent evidence of cyber vulnerability. Consider the recently analyzed GhostNet malware.[4] That malware imported a Trojan horse program onto infected computers which allowed a remote user to, effectively, control the computer. The remote user could activate a keystroke logger, turn on the computer's video camera or microphone, and, of course, exfiltrate any data stored on the computer. First observed on computers operated by the Dalai Lama, the malware was found in dozens of other computers including some located in the embassies of India, Malaysia and Indonesia, ministries of foreign affairs, and even NATO (SHAPE) headquarters (albeit on an unclassified system). Extended analysis eventually traced the malware to an IP address on Hainan Island off the coast of China, an island that, perhaps coincidentally, is home to the headquarters of China's signals intelligence agency.

More prosaically, we know that cyber crime is epidemic and growing. Concrete estimates of the economic costs of cyber crime and cyber intrusions are available and offer some indication of the scope of the problem but are, in some views, highly conjectural. For example, the consulting firm Detica has estimated the annual loss from cyber intrusions in the United Kingdom at £27 billion.[5] Two years earlier, McAfee Security estimated the annual cybercrime losses at $1 trillion globally.[6]

These estimates may well be inflated by their methodology. The lion's share of these losses are estimated to flow from the theft of intellectual property (i.e., some form of industrial espionage) with actual monetary loss estimates running roughly an order of magnitude less (i.e., £3.7 billion annually in the UK from fraud and identity theft).[7] If the same factor were applied to the McAfee global number then the annualized monetary loss worldwide would be $100 billion – a significant number but by no means astronomical. More notably, this data is a rough estimate at best – and they produce figures that are inherently suspect. [Full disclosure: At least one critic, for example, has characterized the Detica study as "nonsense" and "a grubby little piece of puffery."][8]

Perhaps somewhat more authoritatively, the Government Accountability Office, repeating an estimate made by the Federal Bureau of Investigation (FBI), believes that in 2005 the annual loss due to computer crime was approximately $67.2 billion for U.S. organizations. The estimated losses associated with particular crimes include $49.3 billion in 2006 for identity theft and $1 billion annually due to phishing.[9]

---

[4] "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor* (Mar. 29, 2009), http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[5] "The Cost of Cyber Crime," Detica (Feb. 14, 2011), http://www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf.

[6] Elinor Mills, "Study: Cybercrime costs firms $1 trillion globally," *CNet News* (Jan. 28, 2009), http://news.cnet.com/8301-1009_3-10152246-83.html.

[7] "The Cost of Cyber Crime," *supra*.

[8] "Cost of Cyber Crime is not Science Fiction, Says Detica," *Information Age* (May 4, 2011), http://www.information-age.com/channels/security-and-continuity/company-analysis/1621903/cost-of-cyber-crime-is-not-science-fiction-says-detica.thtml.

[9] GAO, "Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats," (GAO-07-705, June 2007). These figures are also broadly consistent with the estimate of $140 billion annual losses made by Ferris

One massive study of Internet traffic conducted for Bell Canada demonstrates both the scope of the problem and the difficulty of definitively assessing its severity. The study reviewed 839 petabytes of data,[10] containing over 4 billion emails each month, carrying more than $174 billion (in Canadian dollars) of commerce every day. Within this flood of data, over 53 gigabytes per second (!) contained malicious code of some sort. The investigators observed on the order of 80,000 zero-day exploits per day and estimated that more than 1.5 million compromised computers attempted more than 21 million botnet connections each month.[11] This data is more or less consistent with estimates by large cybersecurity companies: Symantec, for example, discovered 286 million new, unique malicious threats in 2010, or roughly 9 new malware creations every second.[12] And yet, from all this, the most that can be said is that a large number of financial transactions are at risk – data about actual harm remains painfully elusive.

Cyber Threat Information is a Classic Public Good

Defining a Public Good -- A public good is a good that is both nonrivalrous and nonexclusive.[13] In other words, its use by one person does not affect its use by others and its availability to one person means that it is also available to every other person. The classic example of a public good is national defense. The enjoyment of defense services provided to protect one citizen does not affect the protection enjoyed by another citizen, and defense services provided to one citizen are enjoyed by all other citizens. By contrast, private goods (like, say, a shoe) cannot be used by more than one person (at least at the same time!) and their use by one person affects potential uses by others.

Public goods are, typically, beset by two problems – free riders and assurance. Free-rider problems arise when an individual hopes to reap the benefits of a public good but refuses to contribute to its creation because he thinks others will do so even absent his participation. The assurance problem exists when people refuse to invest in the production of a public good because they believe there will never be enough cooperative investment to produce the good and, thus, that the investment would be futile.

Research, as reported in "Cybersecurity: Where is the Security?" (May 12, 2010), http://www.milesstockbridge.com/pdfuploads/640_Miles_Cyberspace_092410.pdf Phishing is the colloquial phrase used to define efforts to trick unwary to voluntarily disclose their identity and passwords.

[10] This is an immense amount of data. It is roughly 1,000,000 gigabytes and the storage capacity to hold that much data must have cost several hundreds of thousands of dollars.

[11] *Combating Robot Networks and Their Controllers* (Unclassified Version 2.0, May 6, 2010), http://www.scribd.com/doc/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0. One of the authors of the report, Rafal Rohozinski, gave a colloquial talk on this study to the St. Galen Symposium earlier this year. *See* http://www.youtube.com/watch?v=DpRYXRNWka0&feature=youtu.be.

[12] Christopher Drew and Verne G. Kopytoff, "Deploying New Tools to Stop the Hackers," *The New York Times*, June 17, 2011, sec. Technology, http://www.nytimes.com/2011/06/18/technology/18security.html.

[13] *See generally* Paul Samuelson, "The Pure Theory of Public Expenditure" *Review of Economics and Statistics*, 36 (4): 387–389 (MIT Press 1954); David Schmidtz, The Limits of Government: An Essay on the Public Goods Argument (Westview Press 1991).

The classic solution to this conundrum is governmental intervention. When a public good is viewed as necessary but cooperation is unavailing, the government coerces its citizens to cooperate through taxation or some other mandate or incentivizes its creation through a subsidy and thus provides the public good.

Cyber Threat and Vulnerability Information as a Public Good -- Security in cyberspace, like physical security in the kinetic world, is a market good. People will pay for it and pay quite a bit. But, as in the real world, security in cyberspace is not a singular good – rather it is a bundle of various goods, some of which operate independently and others of which act only in combination. Broadly speaking, these goods are purchased in an effort to protect networks, hardware, data in transit, and stored data from theft, destruction, disruption, or delay.[14]

Given the breadth of the scope of the concept of cybersecurity goods, it is unsurprising that different aspects of the bundle may be provided by different sources. Just as some security in the physical world can be purchased directly in the private market, so too in cyberspace many security systems (e.g., anti-virus software and intrusion detection systems) are private goods, bought and sold between private sector actors. They are rivalrous (because their use affects other actors) and excludable (since their owner can limit their use by others). Indeed, evidence from the financial sector suggests that cybersecurity is to a very large degree a private good, adequately provided by the private sector.[15]

There is, however, one aspect of the bundle of cybersecurity goods that appears clearly to be a public good – threat and vulnerability information.[16] That sort of information is both non-rivalrous (giving it to one person to use does not affect how another might use it) and it is non-exclusive (everyone can use the information when it is made available). This public good-like nature of information about cyber threats and vulnerabilities helps to explain the substantial focus of many on laws and regulations regarding information sharing – our legal mechanisms haven't adequately captured the nature of the information being shared and are thought to be an impediment to the wide distribution of this public good, rather than enhancing that activity. It also explains, at least partially, why Google might look to NSA for assistance. They seek a public good, namely information about threats to their systems.

And, of course, this insight into the nature of security information is also consistent with a micro-economic understanding of the incentives that attend the willingness of any individual actor to disclose information about threats and vulnerabilities in its system. There are a host of reasons why private

[14] Eric A. Fisher, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Opinions* 7 (Nova Science Publishers 2009).
[15] Benjamin Powell, *Is Cybersecurity a Public Good? Evidence From the Financial Services Industry*, 1 J.L. Econ. & Pol'y 497, 498 (2005).
[16] Bruce H. Kobayashi, "Private Versus Social Incentives in Cybersecurity: Law and Economics," *in The Law and Economics of Cybersecurity* 16 (Mark F. Grady & Francesco Parisi eds., Cambridge University Press 2006). I am assuming, here, that information is a "good." Some have argued that in the absence of artificial intellectual property protections, information is not a traditional economic good. *E.g.* Murray N. Rothbard, *Man, Economy, and State: A Treatise on Economic Principles 1033* (Ludwig von Mises Institute, Scholar's Ed., 2d. ed. 2009).

sector actors may be reluctant to make such disclosures (especially of vulnerabilities), including: risk of loss of reputation and trust; risk of liability and indemnification claims; negative effects on financial markets; signals of weakness to adversaries; and job security and individual career goals.[17] Treating information as a public good tends to overcome these factors.

The Ambiguity in Current Law

This understanding of the economics of cybersecurity suggests why a significant fraction of the policy debate about cybersecurity and public/private partnerships revolves around the challenge of effective security information sharing. It is often said that existing legal restrictions prevent the private sector from effectively creating cybersecurity. Some of these restrictions are said to relate to the inability of the government to adequately share threat information with the private sector. Other restrictions, more relevant to the subject matter of this Hearing, are said to limit how the private sector shares information with the government or amongst itself.[18]

The focus makes sense when seen through the prism of our theoretical model – because threat and vulnerability information may have the characteristics of a public good, it is affirmatively in society's interests to foster their creation and distribution. If existing laws restrain and restrict either of these, that would be a policy dissonance. On closer examination, many of these legal limitations appear to be less constricting than they are perceived to be. In the end what really restricts cooperation are the inherent caution of lawyers who do not wish to push the envelope of legal authority and/or policy and economic factors (of the sort described above) that limit the desire to cooperate.

The information in question will relate, broadly speaking, either to specific threats from external actors (for example, knowledge from an insider that an intrusion is planned) or to specific vulnerabilities (as, for example, the identification of a particular security gap in a particular piece of software). In both situations, the evidence of the threat or vulnerability can come in one of two forms: either non-personalized information related to changes in types of activity on the network, or personalized information about the actions of a specific individual or group of individuals.[19]

---

[17] E. Gal-Or & A. Ghose, "The economic incentives for sharing security information," *Information Systems Research*, 16 (2), 186–208 (2005).

[18] One important caveat is in order at this point: Information sharing is no panacea. It can, and will, help in preventing attacks where the threat signatures are known. It is ineffective, however, in preventing "zero-day" attacks – that is attacks that are effective on the "zeroth day" because nobody knows about them. In many ways, the problem is very much like the problem with preventing disease – and information sharing is like widely distributing a known, effective vaccine. But no amount of information sharing (or vaccination) can protect you against a brand new virus.

[19] Network traffic information can be information relating to suspicious packets, including ports, protocols, and routing information; specific virus/other malware signatures; IP addresses; and the identification of particularly suspect domains or servers. Personally Identifiable Information (PII) includes more person-specific types of information such as, identifying websites accessed; times and locations of logins/account access; discrepancies in user names; or content of communications and is, more typically, related to a specific malfeasant activity (such as an attempted fraud, identify theft or the transfer of terrorist finances).

Private-to-Private and Private-to-Government Sharing -- Consider the laws that are often said to limit the ability of the private sector to cooperate with the government or amongst itself. Two portions of the Electronic Communications Privacy Act (ECPA),[20] Title I, relating to wiretapping (sometimes spoken of as an amendment to the Wiretap Act),[21] and Title II, relating to the privacy of electronic communications (often called the Stored Communications Act (SCA)),[22] are of facial applicability. These laws were created to protect privacy and to impose checks and balances on law enforcement access to private citizens' communications. As such they serve important public policy goals.

But it is equally true that the laws are of old vintage. Passed initially in 1986, they were largely drafted to address issues relating to the telephone network, and, it is fair to say, have yet to be fully modernized to come to grips with today's Internet-based communications technologies. Some Internet service providers argue that the ambiguous nature of the laws and their applicability prevent them from acting to protect the customers and their networks by making it legally uncertain whether or not they can use certain communications information to protect consumers and/or share certain information voluntarily with the government for purposes of cybersecurity.

Accordingly, they argue, some changes are necessary in law to clearly authorize cooperative cyber activities. The SCA, for example, generally prohibits an electronic communications provider or a remote computing services provider from disclosing the contents of electronic communications or information about a customer who subscribes to its services, absent appropriate legal process. Likewise the Wiretap Act prohibits the interception of communications in transit, except according to legal authorization. The general prohibitions are said to inhibit information sharing of cyber-related threat information.

The arguments for ambiguity are, however, somewhat overstated. Both laws have exceptions reasonably related to the protection of service provider networks. The SCA permits information to be divulged "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service."[23] The phrase has rarely been interpreted (and indeed the one notable case interpreting it involved Apple's argument that it authorized compliance with a civil subpoena, since to fail to do so would cause it to lose money).[24] But there is no reason to suppose that the phrase "protection of property" does not encompass protection of the network that the service provider maintains. To be sure, this requires a slight interpretive leap but it is slight enough that it is difficult to understand the legal hesitancy of network providers on this score.

---

[20] Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848.
[21] Title I is codified at at 18 U.S.C. § 2510 *et seq.* The original Wiretap Act was passed in 1968 as Title III of the Omnibus Crime Control Act.
[22] Title II is codified at 18 U.S.C. § 2701 *et seq.*
[23] 18 U.S.C. §2702(b)(5), (c)(3).
[24] *O'Grady v. Superior Ct.*, 139 Cal.4th 1423 (2006).

Indeed, this "provider protection" language is copied from the provider exception of the Wiretap Act,[25] whose meaning is reasonably well settled. The provider exception of the Wiretap Act gives a provider the right to conduct reasonable, tailored monitoring of the network to protect the provider's property from unauthorized use and for other legitimate provider reasons, as well as to disclose communications intercepted.[26]

Thus, the seeming uncertainty attending the law is rather overblown.[27] There are, however, some real residual questions. The source of the ambiguity lies in the scope and frequency of the information sharing at issue. These provisions permit a "tailored" approach and may not necessarily be read to authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly might be inconsistent with the promise of privacy that undergirds the Wiretap Act and SCA. And yet, routine sharing may be precisely what is necessary to effectively protect the networks. Hence, though the statutory limitations are not as stringent as might be imagined, they do have some effect – and pity the service provider who is trying to determine when his permissibly "tailored" sharing becomes impermissibly "routine."

There are other possible answers of course. For example, both the Wiretap Act and the SCA have consent provisions permitting disclosure or interception in situations where the customer has consented.[28] Relying on these provisions, it would appear that service providers are authorized to collect, use, and disclose communications-related information whenever a subscriber has consented. To

---

[25] 18 U.S.C. § 2511(2)(a)(i).

[26] As a Department of Justice manual details, the provider exception to the Wiretap Act:

> grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service." United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). . . . The exception also permits providers to monitor misuse of a system in order to protect the system from damage or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. See [United States v.] Mullins, 992 F.2d [1472,] 1478 [9th Cir. 1993] (need to monitor misuse of computer system justified interception of electronic communications pursuant to § 2511(2)(a)(i)).
>
> . . . .
>
> [P]roviders investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under § 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to that which is reasonably related to the purpose of the monitoring. See, *e.g.*, United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975) (phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications).

Searching and Seizing Computers and Obtaining Electronic Evidence Manual, ch. 4 (3rd ed. Sept. 2009), http://www.cybercrime.gov/ssmanual/04ssma.html.

[27] Section 314 of the USA PATRIOT Act, may also apply when the private-to-private sharing is done by a "financial institution" (as defined in 31 USC §. 5312(a)(2)). Such institutions are immune from liability for sharing information with each other when, broadly speaking, the information shared is done for the purpose of establishing or maintaining an anti-money laundering program. *See generally* 31 CFR *Part* 103.

[28] 18 U.S.C.§ 2511(2)(c) (Wiretap Act); 18 U.S.C. §2702(b)(3) (SCA).

be sure, there may be ambiguity in the terms of service of existing contracts, but there does not appear to be any barrier to cybersecurity information sharing arrangements if they are, ultimately, grounded on the affirmative, opt-in consent of a customer.[29]

Authorizing Sharing and Legal Uncertainty

The bills pending before Congress go a long way to relieve this uncertainty by explicitly authorizing cyber threat information sharing between private parties and from the private sector to the government. But merely authorizing information sharing will not be sufficient. Simply permitting the sharing will not generate the requisite private sector response if the private sector actor can anticipate adverse collateral consequences.

Why the Hesitation? -- On the private sector side, the reasons for hesitation are clear. Service providers (or more accurately the lawyers for service providers) are inherently cautious and want to avoid litigation and controversy at all costs.

Likewise, there may be good business reasons why a service provider might prefer not to risk collateral consequences such as privilege waivers and the discovery of proprietary information by competitors and critics. Seen in this light then, complaints about the law's ambiguity are also expressions of a desire to have the Federal government, by law, provide liability protection and relieve the service providers of the "ill will" that might attend such an amendment. Trying to avoid litigation and a difficult public relations battle are persuasive reasons for failing to act (though perhaps less so than real ambiguity), and they reflect rational business judgments that provide a good ground for legislation.

The private sector's argument for greater liability protection (and being "authorized" to do the right thing) seems to have carried the political day. The salience of the information-sharing issue was highlighted by the provisions of both the Lieberman-Collins and McCain cybersecurity proposals now pending before the Senate. Both bills clarify that private sector actors are authorized to share information about cyber threats or incidents with the Federal government and with each other. To address the private sector's concerns, the proposal would:

- Affirmatively authorize private sector actors to share information with the Federal government for the purpose of protecting an information system from cybersecurity threats or mitigating such threats;
- Provide private sector actors with civil and criminal immunity for sharing cybersecurity information with DHS; and

[29] There are other ambiguities in the law of lesser general concern relating to the Telecommunications Act of 1934, the Sherman Antitrust Act and, possibly, the Fourth Amendment. For purposes of brevity I will simply say that, as with the ECPA and the SCA the ambiguity is real, though it can be overstated. Perhaps more importantly, there is substantial, significant ambiguity from the application of State laws, many of which impose obligations and limitations that differ from those in the Federal domain.

- Preempt any inconsistent State or local law or regulation that would otherwise prohibit information sharing.

In each of these regards the information-sharing portions of the Lieberman-Collins bill and the McCain proposal closely track the general thrust of the proposal made by the Obama Administration last May.[30] Details, obviously, differ among the three proposals, but the overall thrust is much the same.

Freedom of Information Act Exemptions

Most saliently for this Hearing , both Senate proposals (and the Obama Administration proposal) also include provisions exempting private sector information shared with the Federal government from the ambit of the FOIA. In my judgment that exemption is both wise and essential. If you accept the premise that the cyber threat is real (and I recognize that some may not) then it seems to me that we must resolve any legal uncertainty in favor of enabling information sharing about threats and vulnerabilities. Essential sharing will not occur from the private sector if it is not relieved of the specter of liability and concern that disclosed information will be use adverse to their interests.[31]

The Lieberman-Collins and McCain proposals have, effectively, equivalent FOIA exemption provisions. Section 704(d)(1) of the Lieberman-Collins bill provides that any cyber threat information shared by a private entity with a federal cybersecurity exchange (the new information-sharing structure created by the bill), shall be "exempt from disclosure under section 552(b)(3) of title 5, United States Code, or any comparable State law." Likewise the McCain proposal (in section 102(c)(4)), says that any cyber threat information shared with a Federal cybersecurity center, "shall be deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records." To emphasize the intent of the exemption, the McCain bill further provides (in section 102(c)(5)) for a specific exemption from the OPEN FOIA Act of 2009.[32]

Notably, the consensus about the need for a FOIA exemption is bi-cameral. The Rogers-Ruppersberger bill, H.R. 3523, also provides that any cyber threat information shared with the Federal government is exempt from disclosure under the FOIA. And the Lundgren bill (H.R. 3764) says that information shared with the to-be-created National Information Sharing Organization will, likewise, be exempt from disclosure under FOIA. Not only is the consensus bi-cameral, it crosses branches of government -- the

[30] The language is in §245 of the draft submitted to Congress by the Administration on May 12, 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf.

[31] Much of what I say in this section about the FOIA exemption is also applicable to arguments regarding privilege waiver provisions and prohibitions on the regulatory use of disclosed information.

[32] Section 102(c)(5) requires that information disclosed "shall be, without discretion, withheld from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records."

Obama Administration cybersecurity proposal, in section 245(f) also contains an FOIA exemption that mirrors that in the Lieberman-Collins/McCain/Rogers-Ruppersberger and Lundgren proposals.

Now, some may argue that much of the concern can be answered by the use of existing FOIA exemptions, rather than the blanket provisions of the two pending bills They point out that FOIA already has a bevy of exemptions for national security (5 USC 552(b)(1)), privacy (552(b)(6) and (7)), internal agency decision-making ((b)(5)) and law enforcement ((b)(7)), and suggest that those provisions are sufficient. In my judgment they are inadequate to the task.

First, despite the best intentions, the application of exemptions will, inevitably create greater uncertainty than an absolute prohibition. As the *Milner*[33] case from 2011 demonstrates powerfully, even interpretations of FOIA that have been settled law for a significant period of years are subject to reinterpretation. This potential for ambiguity in the application of FOIA strongly counsels in favor of a blanket exemption .

Second, it is by no means clear whether cybersecurity threat and vulnerability information will fit within one of the existing FOIA exemptions. One can readily imagine types of information (protocol and packet routing information or web-site access logs) that fits in none of these pre-existing categories.

Third, and perhaps more importantly, the application of FOIA in this context seems to me too turn FOIA on its head. The purpose behind the FOIA is to ensure the transparency of government functions. Thus the main ground of a FOIA request is to seek information from the government about the government and its operations. Here, the FOIA exemption contemplated is in relation to private sector information that is not otherwise in the government's possession. We seek the voluntary (*not* compulsory) sharing of this information in order to foster the creation of a clear and manifest public good. But for voluntary agreement of the private sector actors to provide the cyber threat information in the first instance the information would not be in the government's possession and thus not subject to disclosure.

Private sector actors, rightly, would see the absence of an FOIA exemption as a form of government hypocrisy – we need this information, says the government, badly enough that we are asking you to provide it for the common good; but not, says the government in the next breath, so badly that we are unwilling to prevent that information from being shared with other private sector actors who (as your competitors or as your litigation adversaries) might wish you ill.

This, it seems to me, undercuts the very thesis of these information-sharing proposals. If you think (as I do) that sharing of cyber threat and vulnerability information is the most effective (and most cost-effective) way of significantly enhancing the cybersecurity of America's critical infrastructure you cannot, in the same act, turn around and say that the threat information you provide becomes, *pro tanto*, public information.

[33] *Milner v. Dept. of the Navy*, __ U.S. __ (2011), No. 09-1163, http://www.supremecourt.gov/opinions/10pdf/09-1163.pdf.

Finally, let me close this analysis by noting that none of this is to diminish the significance of the FOIA, generally. Transparency is a fundamental and vital aspect of democracy. Those who advance transparency concerns often, rightly, have recourse to the wisdom of James Madison, who observed that democracy without information is "but prologue to a farce or a tragedy."[34]

Yet Madison understood that transparency was not a supreme value that trumped all other concerns. He also participated in the U.S. Constitutional Convention of 1787, the secrecy of whose proceedings was the key to its success. While governments may hide behind closed doors, U.S. democracy was also born behind them. It is not enough, then, to reflexively call for more transparency in all circumstances. The right amount is debatable, even for those, like Madison, who understand its utility.

What we need is to develop an heuristic for assessing the proper balance between opacity and transparency. To do so we must ask, why do we seek transparency in the first instance? Not for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight--it enables us to limit and review the exercise of authority.

In the new cyber domain, the form of oversight should vary depending upon the extent to which transparency and opacity are necessary to the new powers authorized. Here, the proposed legislation would exempt information supplied by businesses regarding cyber attacks from public disclosure. Supplying this information to the government is vital to assure the protection of critical infrastructure. More importantly, allowing public disclosure of such information is dangerous – identifying publicly which cyber threats are known risks use of that information by terrorists and, in turn, draws a roadmap of which threats are not known. Thus, complete transparency will defeat the very purpose of disclosure and may even make us less secure.

What is required is a measured, flexible, adaptable transparency suited to the needs of oversight without frustrating the legitimate interests in limiting disclosure. Here, the public disclosure through FOIA should be rejected in favor of a model of Congressional and Executive Branch review (for example, random administrative and legislative auditing of how the government is using the information provided) that will guard against any theoretical potential for abuse while vindicating the manifest value of limited disclosure.

In short, Madison was not a hypocrite. Rather, opacity and transparency each have their place, in different measures as circumstances call for. The wisdom of Madison's insight--that both are necessary--remains as true today as it was 225 years ago.

---

[34] I first wrote about the thoughts in these concluding paragraphs in Rosenzweig, Calibrated Openness, Harv. Int'l Rev. (Summer 2004).

February 16, 2012

Chairman Joseph Lieberman
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Ranking Member Susan Collins
Senate Homeland Security and Governmental Affairs Committee
350 Dirksen Senate Office Building
Washington, DC 20510

Chairman John Rockefeller
Senate Commerce, Science and Transportation Committee
254 Russell Senate Office Building
Washington, DC 20510

Chairwoman Diane Feinstein
Senate Select Committee on Intelligence
211 Harkin Senate Office Building
Washington, DC 20510

Dear Senators:

On behalf of the undersigned organizations concerned with government openness and accountability, we are writing to let you know of our serious concerns with sections of S.2105, the Cybersecurity Act of 2012, that create unnecessary, overbroad and unwise limitations to access of information, including broad exemptions to the Freedom of Information Act (FOIA), and jeopardize the rights of whistleblowers.

Section 107, as drafted, includes an exceedingly broad definition of "critical infrastructure information," encapsulating information that is crucial for the public to understand public health and safety risks and information already protected under one of the FOIA's other exemptions. Furthermore, the proposed exemption conflicts with Congress' recent effort in the National Defense Authorization Act (NDAA) of 2012 to limit the scope of CII information that can be withheld by the Department of Defense. In the language signed into law this December, Congress rightly recognizes that there can be an overwhelming public interest in disclosing some CII information, and requires the Secretary of Defense to weigh the public interest in disclosure before it can be withheld under FOIA.

Similarly, the language in Section 704(d) relating to cybersecurity threat indicators is troublingly broad, especially considering we do not know what kind of information may be shared in the newly-created cybersecurity exchanges. Cutting off all public access to information in the cybersecurity exchanges before we understand the types of information that may be covered and how best to protect that information while promoting accountability, is bad policy.

We also have concerns about how this bill would limit the lawful disclosures of wrongdoing by whistleblowers. In particular, Section 107(e) would far too narrowly define free speech rights and is not inclusive of existing protections under law. Realistically, whistleblowers will be proceeding at their own risk.

We urge you to not fast track this bill. The unaddressed issues we have identified demand a more careful and thorough consideration. We look forward to working with you to ensure the bill protects our nation's computer networks and promotes transparency and accountability.

Sincerely,

Rick Blum, Coordinator
Sunshine in Government Initiative

Kenneth Bunting, Executive Director
National Freedom of Information Coalition

Angela Canterbury, Director of Public Policy
Project On Government Oversight – POGO

Kevin Goldberg, Counsel
American Society of News Editors

Patrice McDermott, Executive Director
OpenTheGovernment.org

Anne Weismann, Chief Counsel
Citizens for Responsibility and Ethics in Washington

cc: Majority Leader Harry Reid
Minority Leader Mitch McConnell
Senator Patrick Leahy
Senator John Cornyn
Senator Daniel Akaka
Senator Charles Grassley
Senator Carl Levin

March 13, 2012

Chairman John McCain
Ranking Member, Senate Armed Services Committee
228 Russell Senate Office Building
Washington, DC 20510

Dear Senator McCain:

The undersigned organizations dedicated to government openness and accountability are writing to let you know of our serious concerns with provisions of S. 2151, Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act (SECURE IT), that create unnecessary, overbroad and unwise exemptions to the Freedom of Information Act (FOIA).

Section 105 of the bill, titled "Technical Amendments," significantly modifies the FOIA by creating a new exemption that gives the government the authority to withhold information shared with or to a cybersecurity center. This "technical amendment" would be one of the most far-reaching substantive amendment of the Act's exemptions since 1986. Any amendment to the Freedom of Information Act, especially an amendment of this scope, should be referred to the Senate Judiciary Committee, which has jurisdiction over FOIA. Careful consideration by that Committee of FOIA-related legislation, including public hearings, is necessary to ensure that the bill promotes transparency and public accountability while allowing the government to withhold only that information which truly requires protection. Time again over the past quarter-century, proposals to amend the Act's existing exemptions have been rejected as unwise; this proposal, even more dangerously, would add an exemption rather than merely modify one, a fact that itself risks repercussions.

Moreover, Section 105 of the bill refers back to troubling provisions in Section 102 of the bill that expand the authority of the federal government to withhold under the FOIA any and all "voluntarily shared information" given to the cybersecurity centers, create a non-discretionary (b)(3) for all such information, preempt state and local laws, and envision that procedures will be implemented without opportunities for notice and comment.

As drafted, S. 2151 cuts off ***all*** public access to information in cybersecurity centers before the public has the chance to understand the types of information that are covered by the bill. Much of the sensitive information likely to be shared in the cybersecurity centers is already protected from disclosure under the FOIA; other information that may be shared could be critical for the public to ensure its safety. Unnecessarily wide-ranging exemptions of this type have the potential to harm public safety and the national defense more than they enhance those interests; the public is unable to assess whether the government is adequately combating cybersecurity threats and, therefore, unable to assess whether or how to participate in that process.

We look forward to working with you and the bill's cosponsors to ensure the legislation both protects our nation's computer networks and promotes transparency and accountability to the public. If you would like to discuss these issues further, please contact Patrice McDermott, Executive Director of OpenTheGovernment.org, at 202-332-6736 or pmcdermott@openthegovernment.org.

Sincerely,

Alliance for Nuclear Accountability
American Association of Law Libraries
American Booksellers Foundation for Free Expression
American Library Association
American Society on News Editors
Arizona Newspapers Association
Association of Research Libraries
Bahr Law Offices
Bill of Rights Defense Committee
Center for Democracy and Technology
Center for Media and Democracy
Citizens for Responsibility and Ethics in Washington – CREW
Council on American-Islamic Relations – CAIR
Defending Dissent Foundation
Electronic Frontier Foundation
Essential Information
Freedom of Information Center at the Missouri School of Journalism
Government Accountability Project – GAP
iSolon.org
James Madison Project
Mine Safety and Health News
MuckRock
National Coalition Against Censorship
National Freedom of Information Coalition
Nuclear Watch New Mexico
OMB Watch
OpenTheGovernment.org
Progressive Librarians Guild
Project On Government Oversight – POGO
Public Citizen
Public Employees for Environmental Responsibility – PEER
Reporters Committee for Freedom of the Press
Society of American Archivists
Society of Professional Journalists
Sunlight Foundation

Targeted News Service LLC
Tri-Valley CAREs (Communities Against a Radioactive Environment)
Tully Center for Free Speech at Syracuse University
Understanding Government
Utah Foundation for Open Government
Virginia Coalition for Open Government
Washington Coalition for Open Government

Individuals (additional information for identification purposes only)
Mark Tapscott
Editorial Page Editor, Washington Examiner

Tom Kearney
First Amendment chairman, Vermont Press Association

Brian R. Hook
Editor, B.R. Hook and Missouri Journal

Dwight E. Hines, PhD
Peru, Maine

cc: Senator Richard Burr
Senator Saxby Chambliss
Senator Dan Coats
Senator Chuck Grassley
Senator Kay Bailey Hutchinson
Senator Ron Johnson
Senator Lisa Murkowski
Senator Patrick Leahy

○