

# SECRECY REPORT 2013

*Indicators of secrecy  
in the federal government*

This report was made possible by the generous support of the CS Fund, the Open Society Foundations, the Rockefeller Brothers Fund, the Ford Foundation, and the Bauman Foundation.

The authors of this report are Patrice McDermott, Amy Bennett, Abby Paulson, and Shannon Alexander. The report benefited from the helpful advice and assistance of the OpenTheGovernment.org Steering Committee.

## About OpenTheGovernment.org

OpenTheGovernment.org is a coalition of consumer, good government and limited-government groups, environmentalists, journalists, library groups, labor and others united to make the federal government a more open place in order to make us safer, strengthen public trust through government accountability, and support our democratic principles. Our coalition transcends partisan lines and includes progressives, libertarians, and conservatives.

To join the coalition, individuals are invited to read and sign the [Statement of Values](#). Organizations are welcome to visit our site, read the Statement of Values, and contact us if interested in becoming a coalition partner. [www.OpenTheGovernment.org](http://www.OpenTheGovernment.org).

## Steering Committee

Steven Aftergood, Federation of American Scientists  
 Gary D. Bass, Bauman Foundation  
 Tom Blanton, National Security Archive  
 Lynne Bradley, American Library Association  
 Danielle Brian, Project on Government Oversight\*  
 Kenneth Bunting/Thomas Susman, National Freedom of Information Coalition  
 Kevin Goldberg, American Society on News Editors  
 Conrad Martin, Fund for Constitutional Government\*\*  
 Katherine McFate/Sean Moulton, Center for Effective Government (formerly OMB Watch)  
 Michael D. Ostrolenk, Liberty Coalition  
 David L. Sobel, Electronic Frontier Foundation  
 Anne Weismann, Citizens for Responsibility and Ethics in Washington  
 John Wonderlich, Sunlight Foundation

\*Chair \*\* Ex officio member

1100 G Street, NW, Suite 500  
 Washington, DC 20005  
 (202) 332-OPEN (6736)  
[info@openthegovernment.org](mailto:info@openthegovernment.org)

# Secrecy Snapshot

**FOIA REQUESTS INCREASED BY 1%, BACKLOGS DECREASED BY 14%**

**FEDERAL CIRCUIT COURT WHISTLEBLOWER DECISIONS — 3-236 AGAINST WHISTLEBLOWERS**

## CLASSIFIED INFORMATION

*Original Classification Decisions Continue Decline*

*\$199.86 Spent Keeping Secrets for Every Dollar Spent on Declassification*

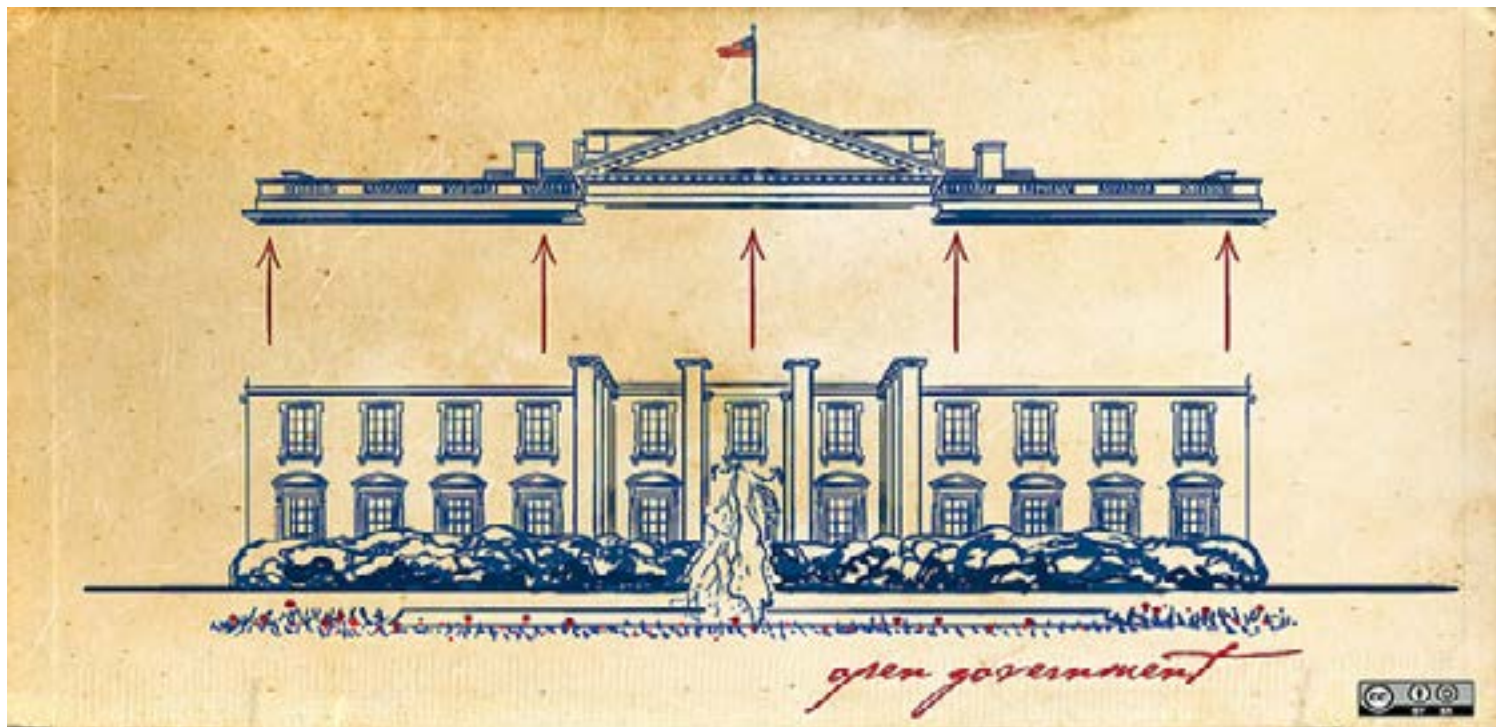
*Mandatory Declassification Requests Drop 27%*

*Classification Challenges Rebound Following 2011 Plunge*

*State Secrets Privilege Policy: Impact Unclear*

*National/Military Intelligence Budgets Disclosed*

**INVENTION SECRECY ORDERS IN EFFECT CONTINUE RISE**



## A Note from OTG's Executive Director

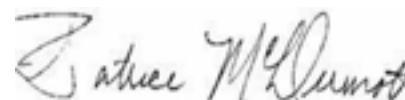
---

We cannot write this Secrecy Report in 2013 without directly confronting the utter disarray in what we thought we knew (and did not know) about the activities of the National Security Agency (NSA), the Department of Justice (DOJ/FBI), and the Foreign Intelligence Surveillance Court (FISC) regarding the collection of information relevant to an investigation to protect against terrorism. The documents disclosed by Edward Snowden (through the Guardian and the Washington Post) were the first shock grenades thrown into the room and the reverberations have continued – and intensified – with the revelations that the national intelligence community (NSA and the Office of the Director on National Intelligence (ODNI) most particularly) have been forced to divulge.

For the last few years we have been reporting on the use of National Security Letters (NSLs) and on the government's applications to the Foreign Intelligence Surveillance Court (FISC). Now, however, we have to question the accuracy and meaningfulness of such numbers and are not including them in this year's Report. Our distrust of the government's reported numbers is focused in four areas: demands for records under Section 215 of the USA PATRIOT Act; the applications made to the FISC under Section 702 of the FISA Amendments Act of 2012; the failure of congressional oversight; and our new understandings of the interactions between the FISC and the intelligence community, and the expanded role of the Court.

These specific concerns are addressed in detail in the following pages. For now, we want to note that while we agree with President Obama that the disclosures made by Edward Snowden are not the optimal way to have started the discussion about the secret law that has allowed startling levels of surveillance of purely domestic communications and digital activities of US persons, we also believe that the discussion would not have occurred otherwise. As a result of the disclosures, the intelligence community has been forced to declassify and release documents that, until recently, [they](#)<sup>1</sup> (and the [FISA Court](#)<sup>2</sup>) averred could not and should not be declassified. The misdirection in which our government has engaged and the use of secret law are, for us, as disturbing as the activities they have hidden.

The secret interpretations of law are the focus of the discussion that follows.\* We are deeply indebted to the many exceptional journalists who are covering these issues and making them comprehensible.\*\*



Patrice McDermott  
 Executive Director  
 OpenTheGovernment.org

---

\* There are important privacy and civil liberties concerns with the NSA and other communications surveillance programs. This report does not focus on them.

\*\*These include Barton Gellman, Ellen Nakashima, Peter Wallsten, Sari Horwitz and William Branigin of the Washington Post; Spencer Ackerman and Glenn Greenwald of The Guardian; Eric Lichtblau and Charlie Savage of the New York Times; Michael Isikoff of NBC News; Conor Friedersdorf of the Atlantic; and also the contributors to the Lawfare Blog, and our colleagues in advocacy.

# 2013 Secrecy Report

---

## Table of Contents

Introduction.....Page 5

Secret Law.....Page 6

Office of the President.....Page 11

Freedom of Information Act.....Page 12

Whistleblowers.....Page 16

Classified Information.....Page 19

Special Section: 5 Big Ideas.....Page 33

Endnotes.....Page 35

This report on trends in secrecy and openness in Fiscal Year 2012 includes data from of the Obama Administration (January 2009 – October 2013). Creating and maintaining open and accountable government requires the committed focus of both the public and the government. What follows is a brief look at how the main indicators we examine have changed over time. Unless otherwise noted, all years are Fiscal Years (FY).

OpenTheGovernment.org issued the first Secrecy Report Card in 2004, chronicling the trends in secrecy and openness in 2003. As readers will recall, that was the year of the U.S. invasion and occupation of Iraq and the third year of the Bush-Cheney Administration. Over the course of that Administration, we charted a significant increase in secrecy which led to a decrease in accountability—to the public and to Congress.

Over the last few years, the reports have generally revealed a trend towards openness as indicators began to creep away from the high-water marks of the mid-2000’s.

### A Note on the Indicators

OpenTheGovernment.org seeks to identify measurable indicators that can be used as benchmarks to evaluate openness and secrecy in government in the United States. We include data based on three criteria:

- data that show trends over time;
- data that have an impact across the federal government or the general public; and
- data that already exist and require little or no further analysis.

These indicators are not intended to be comprehensive; there are additional indicators on secrecy and openness that conceivably could be included. We will continue to adjust the indicators as they fit the focus of this report.

## Introduction

---

On his first day in office, President Obama committed his Administration to creating an unprecedented level of openness in government. Similar to recent reports, this year's Secrecy Report shows that the President's commitment has resulted in some reductions of secrecy according to several of our indicators: agencies continue to make progress in reducing their Freedom of Information Act (FOIA) request backlog; the Office of the Special Counsel, an independent federal investigative and prosecutorial agency that helps protect federal employees from retaliation for blowing the whistle on waste, fraud, abuse, and illegality, has been re-invigorated; the Secretary of Defense, after years of resistance, voluntarily revealed the total amount of money requested for the Military Intelligence Program (MIP); the number of people with the authority to create new secrets continues to drop. This year's report is particularly notable for also charting a significant drop in the extent of newly-classified material.

The change has been slow, though: requesters still have to wait far too long to receive government records; the growing volume of classified material still overwhelms the government's declassification efforts, and far too much material is marked at a classification level beyond its risk to national security. While many of the trend lines may be pointing in the right direction, the rate of change is not enough to create an open and accountable government. For example, documents revealed by Edward Snowden have made all too clear that abuses have resulted from the secrecy surrounding the government's interpretation of the law and of the national security surveillance programs, and the lack of effective oversight of these programs.

As a special section for this year's Secrecy Report, we present 5 Big Ideas to kick-start the kinds of massive changes needed to create noticeable difference in the level of secrecy in the federal government. As we discussed extensively in last year's Secrecy Report, the indicators that we track in our reports are rough indicators of secrecy (and openness) in the federal government, and there is much we do not know (in part because the government will not release, or does not keep, good information). Likewise, the solutions we discuss here are only a sub-set of our larger shared agenda for openness, a set of priorities we have developed in concert with our coalition partners and other allies over the last few years. Although they are not part of our big five here, it is equally important for the Obama Administration to take serious steps to make federal spending transparent; to give the public information to help them know officials are acting ethically and that regulatory decisions are made in the public's interest; to use the state secrets privilege in a way that protects people's right to seek redress in a court of law; and to improve whistleblower protections.

Our annual secrecy report relies on statistics and analyses from the government, journalists, scholarly sources, and our partners. Amid the revelations of secrets, inaccuracies, and misdirections discussed above, we present what we best know to be the indicators of government secrecy and recognize that this field is defined by the unknowns.

# 2012 Trends in Secrecy and Openness

## Secret Law

### Section 215 of the USA PATRIOT Act and National Security Letters

In past years, we have reported on National Security Letters (NSLs). These are written demands from the FBI that compel internet service providers (ISPs), credit companies, financial institutions and others to hand over confidential records about their customers, including, but not limited to, subscriber information, phone numbers and e-mail addresses, web-sites visited.

The letters, which date back to the 1980s, were originally for FBI investigations where there were “specific and articulable facts” indicating the information was related to a foreign agent. The USA PATRIOT Act eliminated the requirements for specific facts and a link to a foreign agent. Section 215 permits the FBI to seek a court order directing a business or other entity to produce records or documents – tangible things – when there are reasonable grounds to believe that the information sought is relevant to an authorized investigation of international terrorism. As long as the head of an FBI field office certifies that the records would be relevant to a counterterrorism investigation, the Bureau can send an NSL request without the backing of a judge or grand jury. That is what the statute says.

However, the broad data collection Verizon was required to provide to the National Security Agency under a recently-revealed [court order](#)<sup>3</sup> was made under the auspices of Section 215. How did we get from “tangible things,” as normally understood, relevant to an authorized investigation of international terrorism, to this?

...the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production on an ongoing daily basis thereafter for the duration of this Order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or “telephony metadata” created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls.

We have recently learned through the [Administration White Paper](#)<sup>4</sup> that multiple FISC judges have found that Section 215 authorizes the collection of telephony metadata in bulk. According to the Administration, the FISC judges consider that the telephony metadata collection program meets the “relevance” standard of Section 215 because there are “reasonable grounds to believe” that this category of data, when queried and analyzed consistent with the Court-approved standards, will produce information pertinent to FBI investigations of international terrorism because

...certain analytic tools used to accomplish this objective require the collection and storage of a large volume of telephony metadata [and] ...communications metadata is different from many other kinds of records because it is inter-connected and the connections between individual data points, which can be reliably identified only through analysis of a large volume of data, are particularly important to a broad range of investigations of international terrorism.

So, the FBI and the NSA are authorized to get this information, not to gain access to specific items about specific persons on a case-by-case basis, but, rather, because technology makes it useful to a “broad range of investigations of international terrorism” – which may or may not themselves have been authorized by the FISC? How did this happen? What we understand of that trajectory is below, but there is still much that we are not sure about.

We have reported in past years on the total number of NSL requests (15,299 in 2012) to the FISC, the percentage of NSL

requests generated from investigations of U.S. Persons (about 41% in 2012), and the number of FISA applications presented and approved for authority to conduct electronic surveillance and physical search (1,788 in 2012). These numbers are contained in letters from the Department of Justice (DOJ) to Congress.

What we did not notice in our readings of these is that the Justice Department was also reporting on Section 215 requests—applications to the FISC “for access to certain business records (including the production of tangible things) for foreign intelligence purposes.” The numbers varied: 43 in 2006, 6 in 2007, 13 in 2008, and 21 in 2009.<sup>5</sup> The numbers of such requests jumped to 96 in 2010, 205 in 2011, and 2127 last year. Of the 212 in 2012, the FISC denied none, but modified two hundred. Then-FBI Director [Mueller’s response](#)<sup>6</sup> two years ago, apparently to a congressional Questions for the Record (QFR), probably accounts for most of the increase in use: beginning in late 2009, certain electronic communications service providers no longer honored NSLs to obtain records because of what their lawyers cited as “an ambiguity” in the law. As a result, Mueller said, the FBI had switched over to demanding the same data under Section 215. According to Mueller, “This change accounts for a significant increase in the volume of business records requests.”

The dramatic increase only tells part of the story, though. Before Snowden leaked the FISC order to Verizon, we assumed – along with nearly everyone else – that this provision was being used in discrete requests to obtain individual collections of records about known counterintelligence or terrorist suspects—“for records showing, say, that a certain person made certain purchases from a certain vendor or used a particular telephone to make specific calls.”<sup>7</sup> In another example of misdirection, the government has, as indicated by the numbers above, suggested that these orders are comparatively rare and focused on specific business records. Indeed, in 2011, the acting head of the Justice Department’s National Security Division (Todd Hinnen), [testified that](#) “. . . Some orders have also been used to support important and highly sensitive intelligence collection operations, on which this committee and others have been separately briefed. On average, we seek and obtain section 215 orders less than 40 times per year.”<sup>8</sup>

We have been distracted with the small numbers (212 Section 215 requests in 2012) and, until now, prevented from knowing that behind those 212 requests were the massive numbers involved in the bulk collections of metadata on calls “wholly within the United States, including local telephone calls.” In addition, we have recently added a new term, “hops,” to our vocabulary. In his testimony before the House Judiciary Committee NSA Deputy Director John Inglis stated that the FISA court “has approved us to go out two or three hops.” The [Washington Post explained](#):

When analysts think they have cause to suspect an individual, they will look at everyone that person has contacted, called the first hop away from the target. Then, in a series of exponential ripples, they look at everyone all those secondary people communicated with. And from that pool, they look at everyone those tertiary people contacted. This is called a second and a third hop.<sup>9</sup>

As members of the committee were quick to point out, this is not what the law as passed by Congress allows.

Regrettably, we should not be surprised by the FISC approval Inglis disclosed, but we should be deeply troubled by another new official disclosure. In an recently declassified and released [85-page ruling](#),<sup>10</sup> Judge John D. Bates, then serving as chief judge on the Foreign Intelligence Surveillance Court, wrote that the court found that its approval of a government interpretation of section 215 of the PATRIOT Act to justify the bulk collection of all Americans’ phone records was “premised on a flawed depiction” of how the program operated and “buttressed by repeated inaccurate statements in the government’s submissions” to the court.

The FISC ruling seems to point to a January 2007 announcement in which the [Justice Department said](#)<sup>11</sup> it had worked out an “innovative” arrangement with the Foreign Intelligence Surveillance Court that provided the “necessary speed and agility” to provide court review of all warrants on all wiretaps in terrorism investigations to monitor international communications of people inside the United States without jeopardizing national security. What these terms meant was made clear at the announcement: a week prior, the Justice Department had obtained multiple orders, or warrants, from the



FISA court allowing it to monitor international communications in cases where there was probable cause to believe one of the participants was linked to Al Qaeda or an affiliated terrorist group . According to then-Attorney General Gonzales, “As a result of these orders any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.” But it now appears that this “innovative” arrangement was “premised on a flawed depiction” of how the program operated and “buttressed by repeated inaccurate statements in the government’s submissions” to the court.

## Section 702 of the Foreign Intelligence Surveillance Amendments Act

We have not reported previously on Section 702 of the 2008 Foreign Intelligence Surveillance Amendments Act. Section 702 permits, the real time bulk collection of Americans’ overseas communications (telephone calls and e-mail, including the associated metadata) as long as the government is targeting foreigners abroad. The section says surveillance may be authorized by the Attorney General and Director of National Intelligence without prior approval by the FISC, as long as minimization requirements and general procedures blessed by the court are followed.

In August, however, we learned that the NSA has not always operated within those strictures. In the [ruling](#) noted above, Judge Bates found that the agency had violated the Constitution and he noted serial misrepresentations to the Court:

The court is troubled that the government’s revelations regarding N.S.A.’s acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

Judge Bates further noted that the collection of purely domestic communications is likely to continue: “NSA has acquired, is acquiring, and if the certifications and procedures now before the Court is approved, will continue to acquire, tens of thousands of wholly domestic communications.” And, indeed, [according to a report](#)<sup>12</sup> about a conference call (about the declassification and release of the ruling), Intelligence Community officials said that the FISA Court paused the program but found that it was “technologically impossible to prevent this from happening.” And that, “The court found the NSA’s procedures for purging wholly domestic communications needed to be beefed up, and that’s what was done.”

As Senator Ron Wyden [has noted](#),<sup>13</sup> though, the ruling exposes the failure of Congress to address what the ruling notes – that the warrantless acquisition of wholly domestic communications, which continues, violates the spirit of the law.

## Issues with Congressional Oversight

It is obvious that something is deeply amiss with congressional oversight of the intelligence community and its activities.

This failure of robust oversight is critical, especially as the [Administration White Paper](#)<sup>4</sup> claims that the Section 215 bulk collection is legal, in large part, because Congress has twice extended the PATRIOT Act without changing the terms of Section 215:

Moreover, information concerning the use of Section 215 to collect telephony metadata in bulk was made available to all Members of Congress, and Congress reauthorized Section 215 without change after this information was provided. It is significant to the legal analysis of the statute that Congress was on notice of this activity and of the source of its legal authority when the statute was reauthorized.

A key of part the argument that the use of Section 215 is legal rests on the Administration’s claim that it gave notice to Congress about the expansion of the program. It is hard to know whether to be as cynical about this issue as the authors of a [Lawfare blog](#),<sup>14</sup> or to believe the [avowals of lack of knowledge](#)<sup>15</sup> by some Members of Congress. From our perspec-

tive, Congress has caved to the demands of the executive branch that only a very small handful of Members (Senators and Representatives) be allowed in on secret briefings to read secret documents – without members of their staffs who are experts on these laws and might be able to ask challenging questions. The Members cannot take notes and cannot speak of what they heard. Rather than conduct oversight, the Congress has accepted the secret assurances of secret agencies about deeply secret programs, and has amended the law to expand the authority of the executive well beyond what even the USA PATRIOT Act did.

There also appears to be a difference in how availability of information about the programs has been handled recently in the Senate and [the House](#).<sup>16</sup> According to the [Washington Post](#)<sup>17</sup>, a declassified document – cited repeatedly by both Administration officials and congressional leaders as assurance of meaningful congressional oversight of the bulk collection of domestic telephone data – was withheld from circulation by the House Intelligence Committee. A cover letter to the House and Senate intelligence committees asked the leaders of each panel to share the written material with all members of Congress. The Senate Intelligence Committee did so. The House Committee opted, instead, to invite all 435 House members to attend classified briefings where the program was discussed — briefings that critics say were vague and uninformative. Justin Amash, the Michigan Republican who led the effort to defund the NSA’s mass phone-records collection, said confronting intelligence officials during the briefings was “like a game of 20 questions,”<sup>18</sup> and added: “If you don’t know about the program, you don’t know what to ask about.”

## The Secrecy of the Foreign Intelligence Surveillance Court and Opinions

The United States Foreign Intelligence Surveillance Court (FISC) was established by Congress and authorized under the [Foreign Intelligence Surveillance Act](#) of 1978 (FISA).<sup>19</sup> FISA and its court (also called the FISA Court) were inspired by the recommendations of a major investigation launched in 1976 by the Select Committee of the United States Senate to Study Governmental Operations with Respect to Intelligence Activities, commonly referred to as the “Church Committee” for its chairman, Senator Frank Church of Idaho. Only the executive branch can submit requests. No one outside government can appear before the FISC judge. Its rulings and its opinions are all secret.

The FISC, whose statutory role is to approve warrant applications for surveillance activities related to national security, seems to have operated for years prior to 9-11 in the manner Congress had intended. Recent revelations raise significant questions about the conduct of the court. Instead of approving warrant applications, FISA court judges are, as noted earlier in regard to Section 215 orders, reviewing and approving bulk collections and “programmatically surveillance”.

Perhaps the greatest change at the FISC is that judges are no longer simply reviewing warrant applications for individual surveillance operations. The authority of the Court has been extended since 2001. It now has the authority to permit the electronic surveillance of entire categories — “without the need for a court order for each individual target”—of non-U.S. persons who are located abroad. Under this provision in the 2012 FISA Amendments Act reauthorization, instead of issuing individual court orders, the FISC approves annual certifications submitted by the Attorney General and the DNI that identify categories of foreign intelligence targets. But while the statutes passed by Congress are available to the public, how those statutes have been interpreted and used remains secret.

The FISC started out (and has continued) as a secret court and, as [Eric Lichtblau has noted](#) “has quietly become almost a parallel Supreme Court, serving as the ultimate arbiter on surveillance issues and delivering opinions that will most likely shape intelligence practices for years to come, according to current and former officials familiar with the court’s classified decisions”<sup>20</sup>

On September 5th, in a [court filing](#)<sup>21</sup> responding to a judge’s order, the Justice Department, said that they would make public a host of material that will “total hundreds of pages” by next week, including:

[O]rders and opinions of the FISC issued from January 1, 2004, to June 6, 2011, that contain a significant legal

interpretation of the government’s authority or use of its authority under Section 215; and responsive “significant documents, procedures, or legal analyses incorporated into FISC opinions or orders and treated as binding by the Department of Justice or the National Security Agency.”

The government says it is “broadly construing”<sup>22</sup> that order and is declassifying a larger set of documents than the ruling requires. It will provide hundreds of pages of documents to the Electronic Frontier Foundation, an Internet civil liberties group and a partner in OTG that had filed a lawsuit under the Freedom of Information Act.

## Recommendations for Curbing Secret Law and Restoring Accountability

The public must have a better understanding of the legal rules under which our government operates and be able to participate in an informed debate about the government’s legal authorities and policies. Congress has introduced several bills that would help meet this goal. The Administration does not have to wait for Congress, however, to curb secret law and help restore the public’s trust in government. Below are our recommendations for steps that the Administration can, and should, take in the coming months. The openness community has submitted these (among other) recommendations to the Administration for inclusion in its upcoming National Action Plan for the Open Government Partnership.

### Authoritative Legal Interpretations and Administrative Opinions

The President should direct the Attorney General to make publicly available copies of documents setting forth the authoritative legal interpretations of the Executive Branch, including operative Office of Legal Counsel (OLC) memos, opinions, papers, etc., that show the extent of executive branch authorities and the rules governing executive branch actions. These documents should be made available with redactions for appropriately classified material as needed. If redacted versions of the documents cannot be made available, then unclassified summaries should be made available.

### FISC and other Secret Judicial Decisions and Opinions

The administration should also make publicly available copies of existing Foreign Intelligence Surveillance Court (FISC) and other secret judicial decisions and opinions, with redactions for appropriately classified material as needed. If redacted versions of the opinions cannot be made available, the administration should urge the FISC to prepare and make available summaries of the opinions.

Other judicial decisions or opinions that include or reflect significant interpretations of the law, such as Electronic Communications Privacy Act (ECPA), should also unsealed and be made available with redactions as needed. If redacted versions of the documents cannot be made available, then unclassified summaries should be made available.

The administration should also make unredacted versions of FISC and other secret judicial decisions opinions and pleadings available to all committees of jurisdiction in Congress.

### Presidential Policy Directives (PPDs)

Additionally, the administration should make publicly available unclassified or summarized versions of classified Presidential Policy Directives (PPDs) that set forth the operative rules and legal guidance for government programs. The administration should promptly inform the public about, and make publicly available in unclassified or (where necessary) redacted/summarized form, any changes to previously published, PPDs. This should include any revocations or modifications, whether express or through practice, of an existing PPD.

## Office of the President

### Signing Statements

While President George W. Bush was not the first President to issue signing statements, he did receive a significant amount of attention and no small measure of criticism for making an unprecedented number of signing statements in conjunction with the enactment of bills passed by Congress. The controversy brought public attention to what was a generally obscure practice, but signing statements themselves, whatever the reasons asserted for their use by a president, remain hard for the public to find and track.

President Obama decried the use of signing statements and the lack of transparency around them as a candidate. However, he has continued to use them, albeit at a lower rate, and has not made them much more transparent. In order to find signing statements issued by President Obama on the White House’s website, the public must sort through an ever-growing list of Presidential statements and releases. Surprisingly, they are not grouped together under “Legislation,” or anywhere else on the site. Fortunately, [a site maintained by Joyce Green](#), a private attorney, makes information about signing statements since 2001 easily available.

Years or Presidencies	Statements Challenging Provisions of Laws
1789-1980	278
Reagan	71
G.H.W Bush	146
Clinton	105
G.W. Bush	161
Obama	20

*Source: Presidential Signing Statements, <http://www.coherentbabble.com/signingstatements/signstateann.htm>; Accessed July 22, 2013.*

In calendar year 2012, President Obama issued a single signing statement. The statement, attached to the Ultralight Aircraft Smuggling Prevention Act of 2012 (H.R. 3801), expressed support for the sponsor, former Representative Gabrielle Giffords, and did not challenge any provisions of the bill.

In his first term, President Obama issued twenty signing statements. Eleven of them challenge specific provisions, eight are ceremonial, and one discusses an inadvertent drafting error in the legislation. This number continues to be significantly lower than previous modern presidents.

## Executive Privilege

As discussed in last year's Secrecy Report, Obama invoked Executive Privilege for the first time\* in June 2012, in response to a subpoena issued by the House Committee on Oversight and Government Reform, chaired by Representative Darrell Issa (R-CA). This is the only time he has claimed the privilege vis-à-vis Congress.

The concept of Executive Privilege, while not explicitly mentioned in the Constitution, dates back to President George Washington who initially refused (but later relented) to provide documents to Congress relating to military defeat in battle with American Indians at the Battle of Wabash in 1791. Washington insisted that the branches of government must be separately maintained.

Several modern-era presidents have asserted the privilege. Perhaps the most famous assertions came from Richard Nixon during the Watergate investigations in 1973 and 1974. But even Nixon only asserted the privilege four times, not completely out of line with his contemporaries.

Assertions to Congress of Presidential Executive Privilege Claims:	
Kennedy	2
Johnson	3
Nixon	4
Ford	1
Carter	1
Reagan	3
G.W.H. Bush	1
Clinton	5
G.W. Bush	6
Obama	1

## THE FREEDOM OF INFORMATION ACT (FOIA)

The Freedom of Information Act is the public's strongest tool for accessing information about the government. However, the demands of the process and roadblocks embedded within it have resulted in agency backlogs.

In FY 2012, the federal government received and processed a record number of requests. The number of requests received increased by one percent, to 651,254. The number of requests processed in FY 2012 increased by an even greater percentage (five percent from FY 2011), and the number of requests processed exceeded those received by about two percent in FY 2012.

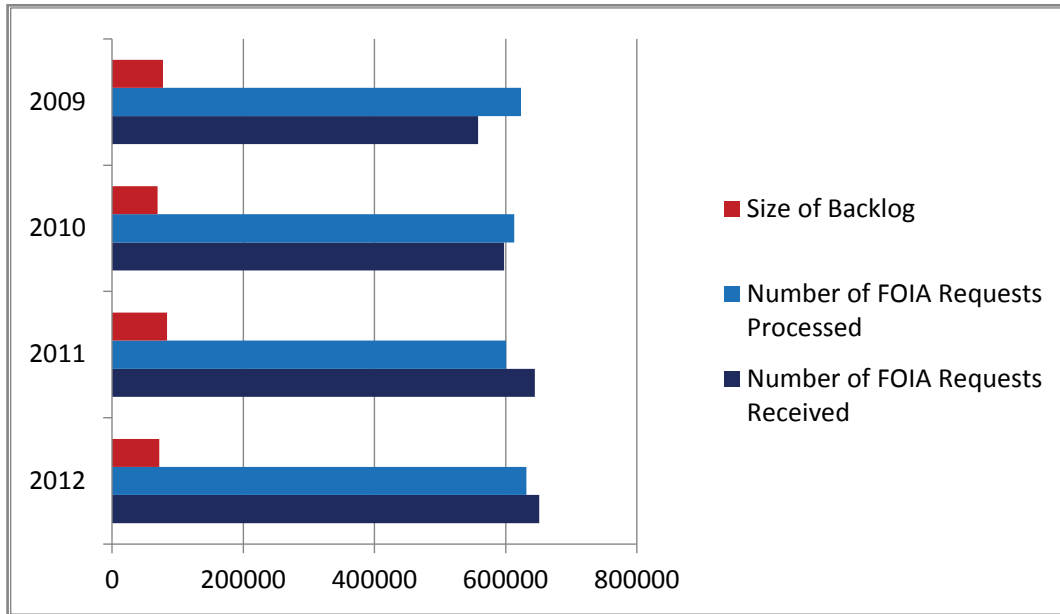
Agencies also decreased the overall FOIA backlog by 14 percent. The backlog is the number of requests that federal agencies have not responded to by the 20-day deadline set by the law.

**“You’re talking about such large backlogs and such slow processing that to some extent these improvements are sort of like spitting into the ocean.”**

**VIDEO:** Kevin Goldberg of the American Society of News Editors (ASNE) discusses whether these changes in processing are felt by requesters.

\*Vis-à-vis Congress; in litigation, the Administration has relied on aspects of executive privilege.

## Processing Increases, Backlog Decreases in FY 2012



\* Statistics in this graph only include data from 2009 to present because prior to 2009 some agencies also included Privacy Act requests in their annual FOIA reports.

**“I want to make it easier to file FOIA requests. Ideally, we would make it easier to get information without having to file a request.”**

**Video:** Goldberg outlines possible improvements to FOIA processing.

**“The FOIA processing times and backlogs are still way too long...most agencies are still having trouble even making the statutory requirements. For a journalist that makes the use of the law very untenable.”**

**Video:** Goldberg discusses the impact of long processing times on journalists.

## Public Requests under the Freedom of Information Act

Fiscal Year	Number of FOIA Requests Received	Number of FOIA Requests Processed	Size of Backlog
2012	651254	665924	71790
2011	644165	631424	83490
2010	597415	600849	69526
2009	557825	612893	77377

Source: *Summary of Annual FOIA Reports*; 2012 statistics accessed 7/22/2013.

Administrative appeals (of withheld information) increased government wide by 11 percent, to 11, 899. Although the government overall processed 10 percent more appeals in 2012 (11, 789), the backlog of administrative appeals increased to 3,120.

A three-year trend of increasing FOIA staff government wide was broken as the number of full-time FOIA staff across government decreased by 7.5 percent in 2012. OIP largely attributes the decrease to a reduction of staff at the Department of Defense.

### Increased Use of Exemption 5

In last year’s summary of agency annual FOIA reports, the Department of Justice highlighted the three years of steady decrease in the use of exemption 5. This trend came to a screeching halt in 2012 with an increase that almost erases the decreases of the previous three years: exemption 5 was used 79,474 times in FY 2012, an increase of approximately 41% over 2011 (56,267). It is worth noting, though, that even with this startling increase, the assertion of this exemption is lower than in FY2009, which mostly fell during the final year of the G.W. Bush administration.

Exemption 5 of the FOIA permits nondisclosure of “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.” According to the [Department of Justice FOIA handbook](#)<sup>27</sup>, the “most frequently invoked privileges incorporated in the exemption are the deliberative process privilege, attorney work-product privilege, and the attorney client privilege.”

**“The big problem is this is an exemption that is difficult to attack in court...the government gets a lot of deference in regard to exemption 5.”**

**VIDEO:** Kevin Goldberg (ASNE) discusses the large increase in the use of exemption 5.

## The Cost of FOIA

The amount of money spent processing FOIA requests overall decreased by approximately 1.7 percent to \$405,464,199.93. The amount spent per request fell by \$44.65.

Year	Cost of Processing FOIA Requests	Number of Requests Processed	Cost / Request Processed
2010	\$394,222,134.00	600849	\$656.11
2011	\$412,647,829.50	631424	\$653.52
2012	\$405,464,199.93	665924	\$608.87

**“The number one thing that has to happen with FOIA reform is...a dedication of financial resources to the FOIA process.”**

**VIDEO:** Kevin Goldberg outlines what's needed to truly reform the FOIA process.

## Records Management

The proper management of government records, most particularly electronic records (including e-mail), is central to accountable government. Without appropriately saved and managed records, neither meaningful FOIA or effective management of the executive branch can be assured, nor is history of government possible. Currently, the risk of loss of electronic records is profound and the management of government e-mail as records is dismal, to say the least. Without good management of records, unintentional secrecy is a probable by-product and deliberate secrecy-by-destruction is likely.

On November 28, 2011, President Obama signed the [Presidential Memorandum -Managing Government Records](#)<sup>28</sup>, followed on August 24, 2012, by M-12-18 — [Managing Government Records Directive](#)<sup>29</sup>, issued by the Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA). Part I of the Directive pertains to federal agency requirements and sets out two goals: agencies are required to work towards implementing electronic recordkeeping by 2019; and agencies must demonstrate compliance with Federal records management laws and regulations. The first goal includes firm time frames for agencies to manage all permanent electronic records in an electronic environment (by 2019) and all e-mail records in an electronic environment (2016). The second goal emphasizes federal records management laws and regulations covering agency responsibilities for identifying and transferring permanent records and scheduling all their records. Each agency must designate a Senior Agency Official (SAO), at the level of Assistant Secretary or equivalent, who is responsible for meeting the overall requirements of the Directive and ensuring the compliance and the success of the agency records management program.

Some\* of the impetus for the Directive has come from the [Records Management Self-Assessment](#)<sup>30</sup> reports over the last 4 years; these present the results of the annual NARA records management self-assessment (RMSA) taken by Federal agencies. The goal of RMSA is to determine whether Federal agencies are compliant with statutory and regulatory records management requirements. Each responding agency receives a numerical score between 0-100 and is placed into Low, Moderate, and High Risk Categories based on those scores. These categories measure how effectively government records are managed. In the 2012 report, the majority of agencies continue to score in the Moderate to High Risk Categories (of compromising the integrity, authenticity, and reliability of their records, and of their loss), but NARA notes movement upward in scores within these categories.

\*The openness community has been promoting the issue of electronic records management for at least 20 years.



## WHISTLEBLOWERS

### OFFICE OF SPECIAL COUNSEL (OSC)

The OSC, on which we are reporting for the second time this year, is an independent federal investigative and prosecutorial agency. Its primary mission is to safeguard the merit system in federal employment by protecting covered employees and applicants from prohibited personnel practices, especially reprisal for whistleblowing. The Office of Special Counsel reported its FY 2012 case activity and results in the [FY 2014 Congressional Budget Justification](#).<sup>31</sup>

The agency provides a secure channel for disclosures, by covered\* federal employees and applicants, of wrongdoing in government agencies.\*\* Federal employees, former federal employees, or applicants for federal employment may disclose violations of law, rule or regulation; gross mismanagement; gross waste of funds; abuse of authority; or a substantial and specific danger to public health or safety. Many disclosures involve complex and highly technical matters unique to an agency's or a whistleblower's duties, such as disclosures about aviation safety, engineering issues, and impropriety in federal contracting.

The OSC received 23.6 percent more new disclosures in FY 2012 than 2011.

**“We’re seeing...a real invigoration of the agency. More people have faith reporting to the agency, and the numbers you see in the Secrecy Report reflect that.”**

**VIDEO:** *Danielle Brian of the Project On Government Oversight talks about the OSC’s increasing value.*

**“In some of the cases currently what we’re seeing is [the Espionage Act] being used to prosecute people who are trying to inform the public, American citizens, on its own government’s activities.”**

**VIDEO:** *Brian discusses the chilling effect of the Espionage Act.*

\*Someone who is covered by the merit system as part of the civil service system, as provided under 5 USC 2302(a)(2)(B) and (C). Excluded employees are also identified there.

\*\*Additionally, it enforces and provides advice on Hatch Act restrictions on political activity by government employees, and enforces employment rights secured by USERRA for federal employees who serve their nation in the uniformed services.

**Summary of Whistleblower Disclosure Activity: Receipts and Dispositions**

Fiscal Year	2006	2007	2008	2009	2010	2011	2012
Pending disclosures carried over	110	69	84	128	125	83	132
New disclosures received	435	482	530	724	961	928	1,147
Total disclosures	545	551	614	852	1086	1011	1,280
Disclosures referred to agency heads for investigation and report	24	42	40	46	24	47	39
Referrals to agency IGs	10	11	9	10	2	5	6
Agency head reports sent to President and Congress	24	20	25	34	67	22	36

**Results of Agency Investigations and Reports**

Disclosures substantiated in whole or in part	21	19	22	30	62	21	31
Disclosures unsubstantiated	3	1	3	4	5	1	5
Disclosures processed and closed	478	467	488	727	1006	870	1,053

In FY 2012, the Office of Special Counsel secured 159 favorable actions for federal employees who have been victims of reprisal for whistleblowing or other prohibited personnel practices — an 89% increase over FY 2011 (83) and an all-time high for the agency. The previous high was 92 favorable actions in 2010.

**Summary of All Prohibited Personnel Practice Complaints Received**

Fiscal Year	2006	2007	2008	2009	2010	2011	2012
Pending Complaints-Carried over	521	386	358	474	769	863	934
New Complaints Received	1805	1970	2089	2463	2431	2583	2969
Total Complaints	2326	2356	2447	2937	3200	3446	3903

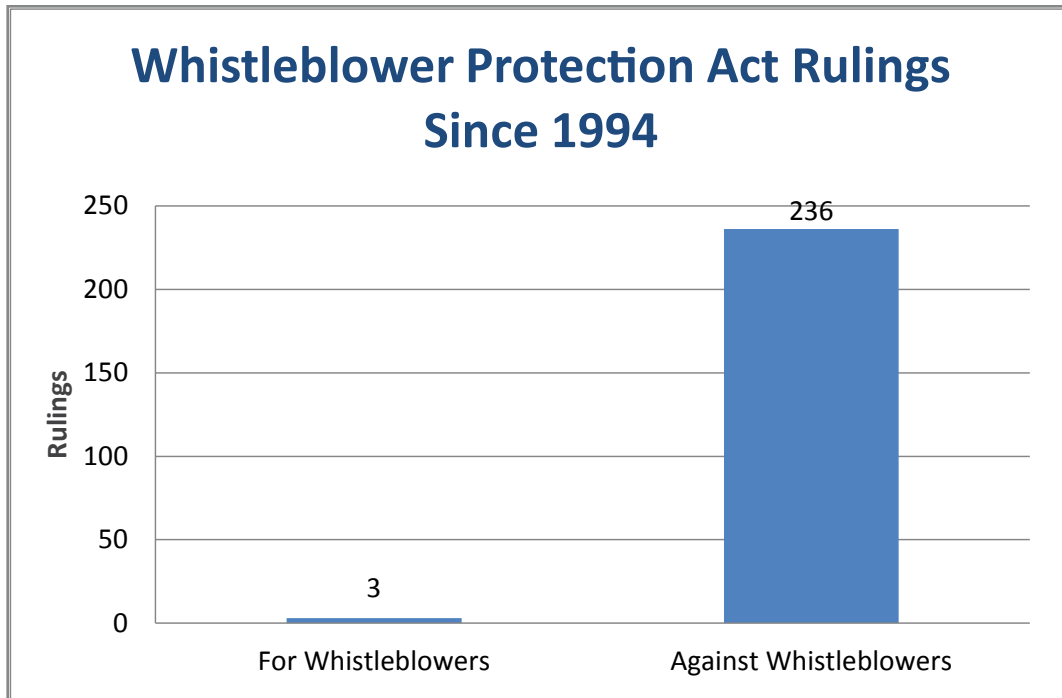
## Federal Circuit Court Continues to Rule against Whistleblowers

Federal whistleblowers still face daunting odds, however, at the appeals court that has a monopoly on reviewing Whistleblower Protection Act cases, the Court of Appeals for the Federal Circuit. Since Congress passed amendments strengthening the Whistleblower Protection Act in October 1994, the track record of all Federal Circuit whistleblower decisions is 3-236 against whistleblowers. An [analysis by Tom Devine](#)<sup>32</sup> of the Government Accountability Project of 181 of the cases shows the numbers of times the court established rulings against whistleblowers and the elements on which the rulings were based:

- Protected speech (whether the employee is entitled to any reprisal protection for his or her disclosures)—93 cases;
- Knowledge (whether an official with responsibility to recommend or take a relevant personnel action knew or should have known of the whistleblowing disclosure)—15 cases;
- Nexus (whether the disclosure was a contributing factor to alleged discriminatory treatment the employee is challenging)—34 cases;
- Clear and convincing evidence (whether the disclosure was a contributing factor to alleged discriminatory treatment the employee was challenging)—39 cases.

The Whistleblower Protection Enhancement Act (WPEA) was signed into law in November 2012. The law expanded protections for federal employees against retaliation and closed loopholes that had previously left whistleblowers vulnerable. The administration issued Presidential Policy Directive 19 in October 2012 to extend many of the protections to national security and intelligence whistleblowers. In July 2013, the U.S. Merit Systems Protection Board expanded the WPEA to retroactively grant anti-retaliation protections to whistleblower cases pending before the WPEA’s passing.

Members of Congress and whistleblower advocates expressed concern that [President Obama’s signing statement](#) on the National Defense Authorization Act of FY 2013 undermined the protections in the WPEA and NDAA. The implementation of the law and its impact will take time to surface.



## CLASSIFIED INFORMATION

The numbers we provide below give a sense of the process of government secrecy, but not necessarily the legitimacy of the asserted secrets. Classified records may be secrets in legitimate need of protection. Some designations, however, are revealed to be frivolous or intended to cover wrongdoing or embarrassing information—even though Executive Order 13526 says this is impermissible.

### State Secrets Privilege

In September 2012, the Obama administration renewed its state secrets claim in *Jewel vs. NSA*<sup>33</sup>, first asserted in this case in 2009. The case, filed by the Electronic Frontier Foundation (EFF)\* on behalf of AT&T customers, challenges the communications surveillance programs conducted by the National Security Agency. In July 2013, a judge in the US District Court of Northern California rejected the government’s claim, asserting that the subject of the lawsuit—the classified surveillance programs—was not a state secret and that properly classified matters could be litigated under the Foreign Intelligence Surveillance Act.

Other than this victory, it appears that the *Department of Justice 2009 policy*<sup>34</sup>, creating an internal review process for assertions of the state secrets privilege, has yet to have significant apparent effect on the Administration’s decision to invoke the privilege.

The use of the state secrets privilege has frustrated judicial redress for constitutional wrongdoing, including government assassination, torture, kidnapping, illegal surveillance. Congress is empowered to and should force the Executive Branch to choose in civil cases (as they are in criminal cases under the Classified Information Procedures Act) to either disclose relevant classified information necessary to litigate the case fairly or accept a default judgment as to liability (with damages to be proven).

Years (inclusive)	1953–1976	1977–2000	2001–12/2008	2009—2012
Times Invoked in Cases	6	59	48	9
Period (in years)	24	24	8	4
Yearly Invocations (avg.)	0.25	2.46	6	2.25

Source: We search on the [US Department of Justice site](#) and use news accounts to identify re-assertions and new assertions. Other, more *exhaustive, methodologies\** yield different results. The counts indicate that the use of the state secrets privilege by the federal government rapidly accelerated in recent history, but have decelerated in the current Administration.

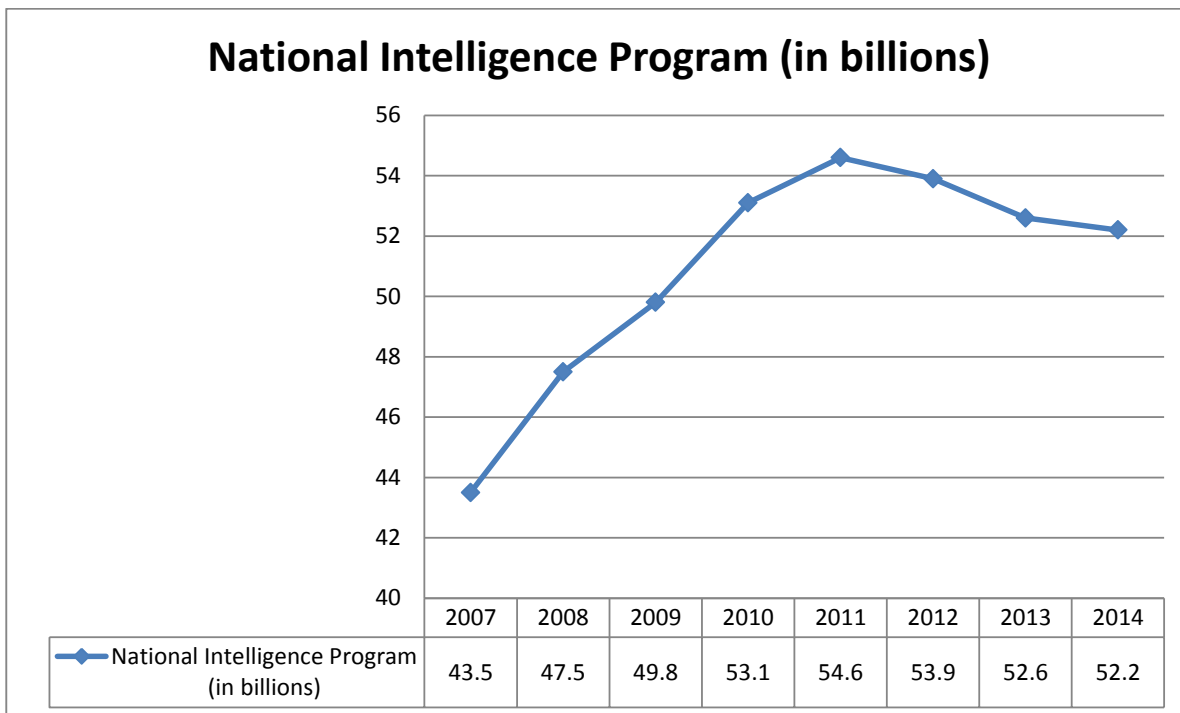
\*An OpenTheGovernment.org coalition partner.  
 \*\*Notably, the Georgetown Law State Secrets Archives.

## Intelligence Spending

The official disclosure of intelligence budget figures continues to be among the outstanding success stories in the quest for open government, particularly because such disclosure was resisted by government officials for so long. While Congress had mandated disclosure of the National Intelligence Program (NIP) request, which was revealed for the first time in 2011, there was no legal requirement to release the Military Intelligence Program (MIP) request. In February 2012, the Secretary of Defense voluntarily disclosed the 2013 MIP request anyway, despite DoD having refused a FOIA request for the same information two months previously. DoD classification officials subsequently reconsidered their position and concluded that disclosure of the MIP budget request would not damage national security and therefore should not be classified.

The disclosure of these budgets provides limited insight into intelligence spending that, according to a September 2013 [Congressional Research Service report](#)<sup>35</sup>, “has roughly doubled since the September 11, 2001, terrorist attacks and, before declines over the last three years, was almost double spending at its peak at the end of the cold war.”

The publicly-released appropriations request for the National Intelligence Program for FY 2014 is \$52.2 billion,<sup>36</sup> a slight decrease from 2013’s request. The Department of Defense publicly released an [MIP FY 2014 request](#)<sup>27</sup> for \$18.6 billion, also a slight decrease from FY 2013’s. In both cases, this is only the portion of the request that has been determined to not jeopardize any classified activities. In August 2013, The Washington Post published details from the FY 2013 Congressional Budget Summary for the National Intelligence Program. The document, obtained by the Post through Edward Snowden, provides a more detailed insight into the objectives of the \$52.6 billion classified budget divided among 16 spy agencies.



## Security Clearance Numbers Appear to Grow; Exact Number Still Murky

For the past three years, the number of security clearances has served to indicate the growth of the classified universe. As of October 1, 2012, 4,917,751 personnel<sup>38</sup> were deemed eligible for clearance, a 1.1 percent growth from 2011. These numbers do not provide a clear picture, though, of the scope of individuals with access to classified information. The Office of the Director of National Intelligence (ODNI) is required to report on the number of personnel “deemed eligible” for clearance, not the number of personnel granted access to classified information. Cleared employees are given access on a “need to know” basis.

As Steven Aftergood of the Federation of American Scientists [noted](#), it is unclear if this is the largest the security system has ever been. Until 2010, the growth of the security system was only estimated by the Government Accountability Office: its 2009 estimate of 2.4 million clearances turned out to underestimate the number by 50 percent.

## Source of Secrets Continues to Shrink: 2,362 “Original Classifiers”

President Obama’s December 29, 2009 Executive Order (EO) on Classified National Security Information<sup>39</sup> (13526) directed all agencies to review their delegations of Original Classification Authority (OCA). An “original classification authority” delegation gives federal workers authorization to create a new memo, analysis, or report and to “originally” classify the information contained in the document as either “top secret,” “secret” or “confidential.” Original classification decisions are the “sole sources of newly classified information.”

The required review was completed by all agencies in 2010. The number of OCAs, which dropped significantly in 2009, has continued to drop steadily since, from 2,362 in 2011 to 2,326 in 2012.

## Classification Decisions

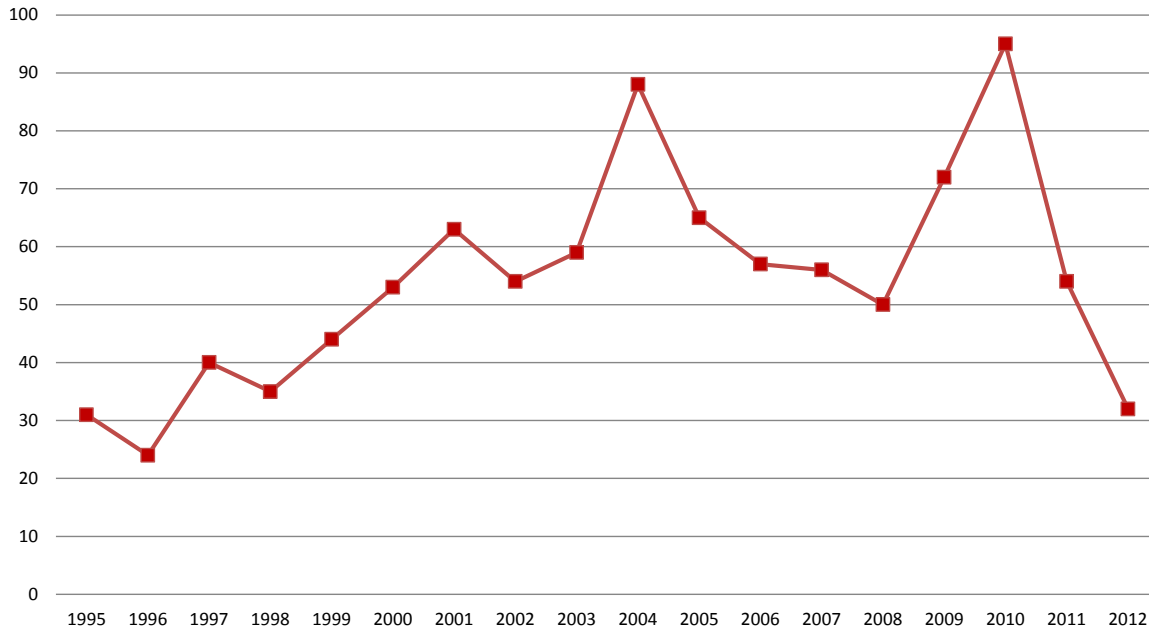
### *Original Classification Decisions*

Original classification activity continued to fall in 2012, accompanied by the small decrease in the number of classification authorities noted above. OCAs made 73,477 original classification decisions—a 42 percent decrease from 2011 and a 67 percent decrease since 2010. The Information Security Oversight Office (ISOO), in its [Report to the President](#),<sup>40</sup> attributes the decreases in part to the recently completed Fundamental Declassification Guidance Review. This process required agencies to update classification guides to ensure the guidance reflects current circumstances and to identify classified information that no longer requires protection and can be declassified.

**“Although there have been some promising reductions in the secrecy statistics in the past year, in most cases they are too small and the amount of secrecy is too big for the public to really sense a difference.”**

**VIDEO:** Steven Aftergood addresses whether the public will feel the effects of the decline of classification activity and number of original classifiers.

### Classification Activity per Original Classifier Falls



### Classification Activity in the Federal Government

Year	Original Classifiers	Original Classification Decisions	Average Classification Activity per Original Classifier
1995	5379	167840	31
1996	4420	105163	24
1997	4010	158733	40
1998	3903	137005	35
1999	3846	169735	44
2000	4130	220926	53
2001	4132	260678	63
2002	4006	217288	54
2003	3978	234052	59
2004	4007	351150	88
2005	3959	258633	65
2006	4042	231995	57
2007	4182	233639	56
2008	4109	203541	50
2009	2557	183224	72
2010	2378	224734	95
2011	2362	127072	54
2012	2326	73477	32

Source: Information Security Oversight Office (ISOO). 2012 Report to the President.

## Good-Faith Classification Challenges Jump

Executive Order 13526 encourages authorized holders of classified information to challenge the classification status of information that they believe, in good faith, to be improperly classified. The number of such challenges has greatly fluctuated over the years: in 2011 challenges dropped nearly 90 percent from 2010 but increased by more than 400 percent from 2011 to 2012.

The current classification status of information was overturned in part or in full 126 times (31.3 percent) in 2012. Ten challenges are pending.

## The Cost of Secrecy Slightly Shrinks

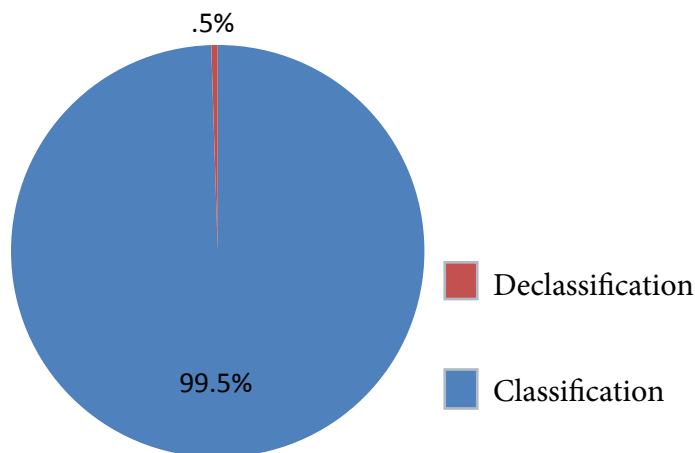
In 2012, the government spent 14 percent less on securing classified information, but also 7.6 percent less on declassification. Overall, government agencies spent \$9.77 billion to secure classified information: \$1.59 billion on securing secrets; and only \$48.65 million on declassification.

While the publicly-reported total sum of classification-related costs and amount spent on declassification both declined\*, the percentage of overall funds spent on declassification remained miniscule — only 0.5 percent. Looked at the other way, for every \$1 spent on declassification, the government spent nearly \$200 on protecting information designated secret.

“There are lots of areas of important public policy debate that are fenced off by secrecy rules.”

VIDEO: *Aftergood* defines overclassification.

### 2012 Classification Costs



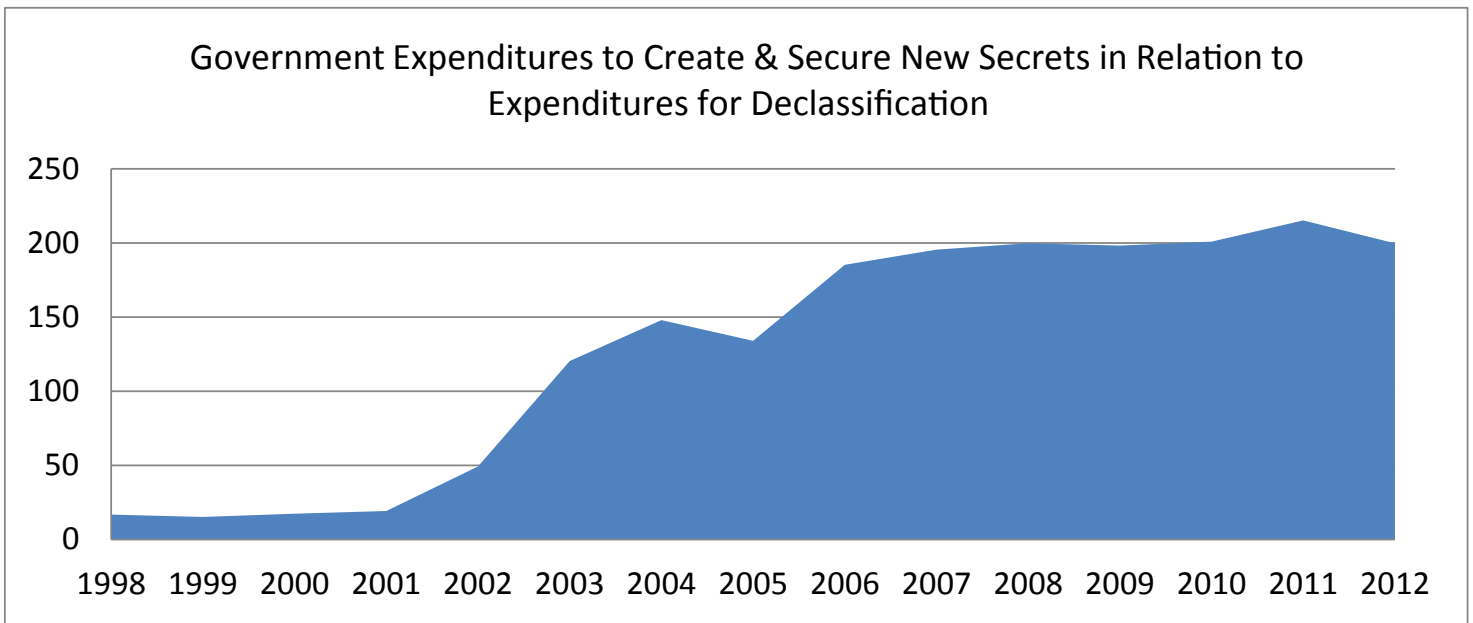
\*The publicly-reported numbers on the amount spent on declassification include, for the most part, only the cost of the people engaged and the equipment, not the cost of physical security and personnel security. These overhead costs are shared, and agencies are not required to separate their figures.



**FEDERAL EXPENDITURES ON CLASSIFICATION AND DECLASSIFICATION  
 IN MILLIONS (excluding CIA, NGA, DIA, NSA and NRO)**

Fiscal Years	Cost of Securing Classified Information	Portion Spent on Declassifying Documents	Classification Costs Per \$1 Spent on Declassification
1997	\$3,380,631,170	\$150,244,561	\$22
1998	3,580,026,033	200,000,000	17
1999	3,797,520,901	233,000,000	15
2000	4,270,120,244	230,903,374	17
2001	4,710,778,688	231,884,250	19
2002	5,688,385,711	112,964,750	49
2003	6,531,005,615	53,770,375	120
2004	7,200,000,000	48,300,000	148
2005	7,700,000,000	57,000,000	134
2006	8,200,000,000	44,000,000	185
2007	8,650,000,000	44,000,000	195
2008	8,640,000,000	43,000,000	200
2009	8,813,475,271	44,650,000	196
2010	10,169,149,557	50,442,266	201
2011	11,360,000,000	52,760,000	215
2012	8,031,491,723	48,651,054	200

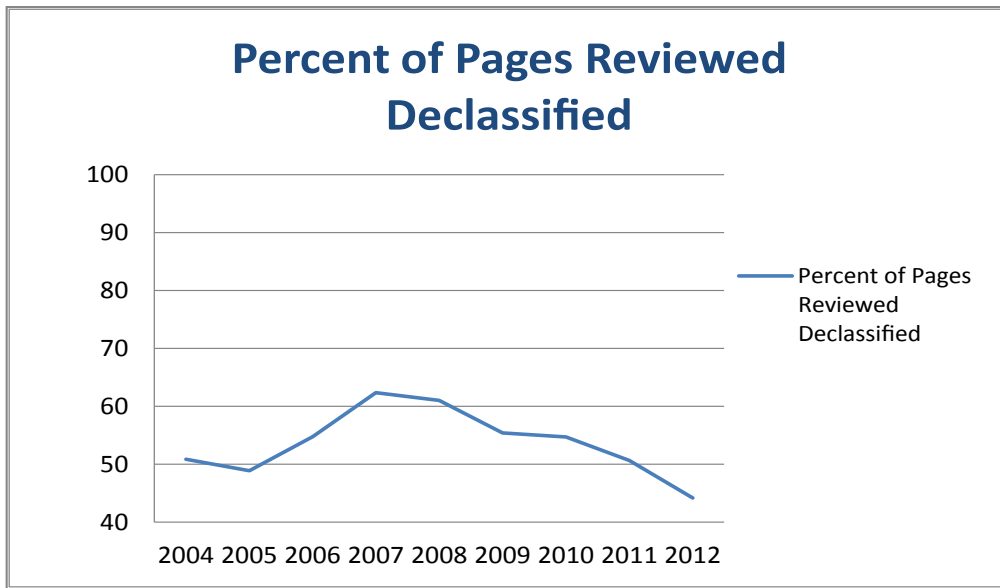
Source: OpenTheGovernment.org calculations based on data from the Information Security Oversight Office (ISOO). 2012 Report to the President



## Overall Declassification Efforts Decline

In FY 2012, 44.92 million pages— 7,838,660 fewer than FY 2011— were reviewed for declassification through the automatic, systematic, and discretionary programs. While agencies in 2012 reviewed 45 percent more pages than the previous year, the ISOO report notes that, overall, agencies reviewed nearly 8 million fewer pages under the combined automatic, systematic, and discretionary declassification reviews than in 2011. ISOO cites changes in contractors, a temporary loss of access to the Washington National Records Center, and the relocation of facilities as some of the factors contributing to the decline. ISOO also notes that agencies conducted a large one-time declassification review in 2011, causing a spike in the declassification activity in that year.

As of December 30, 2012 the NDC had released<sup>41</sup> 57 million pages to the public, a 61 percent release rate. Of the pages reviewed elsewhere in the government, 44 percent (19.85 million pages) were declassified— a drop of 7 percent from FY 2011, during which release rate was 51 percent.

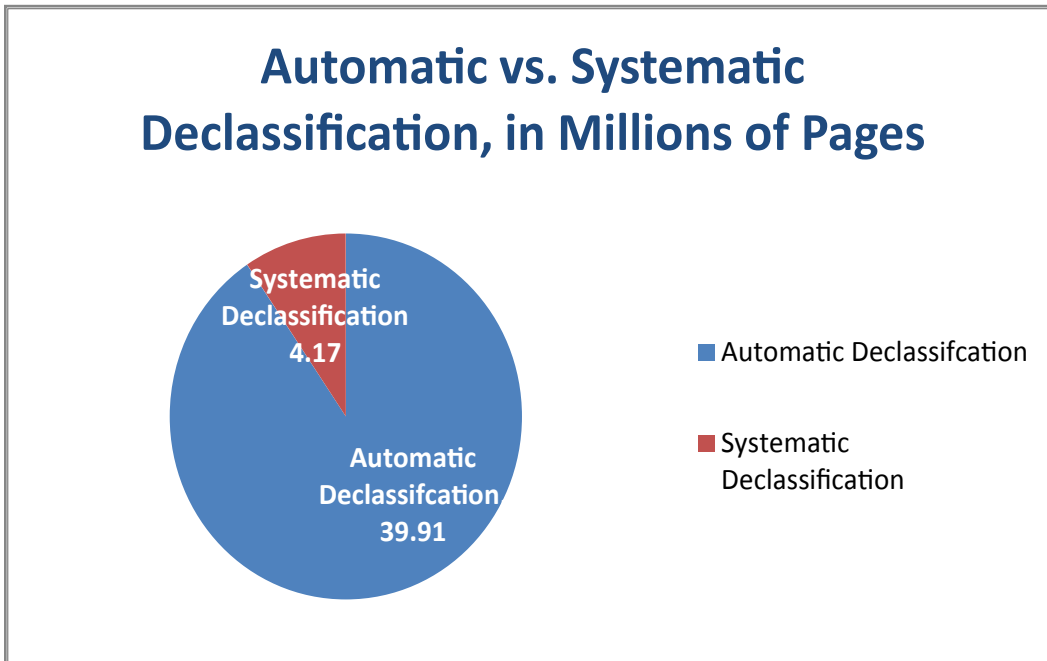


Fiscal Year	Number of Pages Declassified
1995	69,000,000
1996	196,058,274
1997	204,050,369
1998	193,155,807
1999	126,809,769
2000	75,000,000
2001	100,104,990
2002	44,365,711
2003	43,093,233
2004	28,413,690

2005	29,540,603
2006	37,647,993
2007	37,249,390
2008	31,443,552
2009	28,800,000
2010	29,050,290
2011	26,720,121
2012	19,850,541

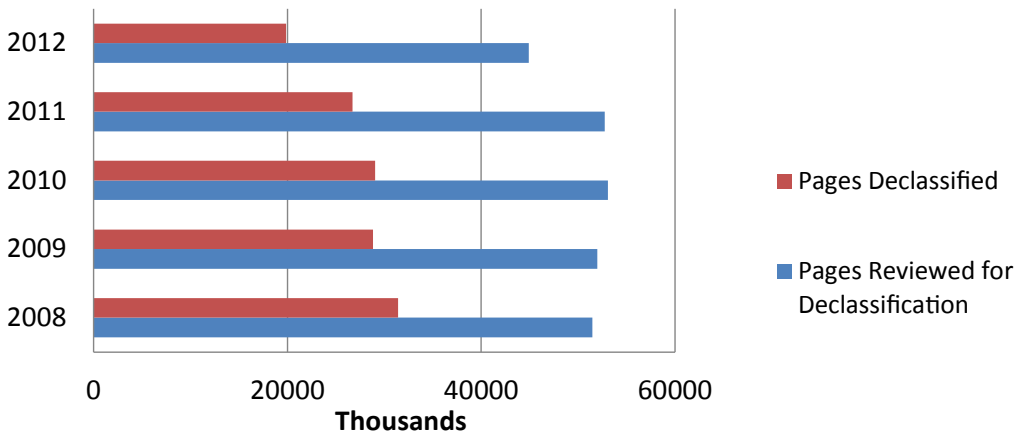
### Automatic and Systematic Declassification Review\*

Automatic declassification accounted for 88.8% (39.91 million pages) of the 44.92 million pages reviewed and 89.1 % (17.69 million pages) of the 19.85 million pages declassified in 2012. Systematic declassification accounted for 4.17 million pages reviewed and 1.98 million pages declassified. Under discretionary declassification review, 846,915 pages were reviewed and 179,186 pages were declassified.



\*E.O. 13526 continues the requirement that all agencies automatically declassify information that has “permanent historical value,” unless the information falls under several limited exemptions allowing continued classification. After several deadline extensions, automatic declassification came into effect on December 31, 2009. The E.O. also requires agencies to create and maintain a viable systematic review of records less than 25 years old and those exempted from automatic declassification, and to prioritize review based on researcher interest and the likelihood of declassification. Automatic declassification review and systematic declassification review are combined in the data ISOO collected from 1996 through 2009. For 2010, ISOO provided separate numbers for automatic and for systematic declassification.

## Automatic and Systematic Declassification Review

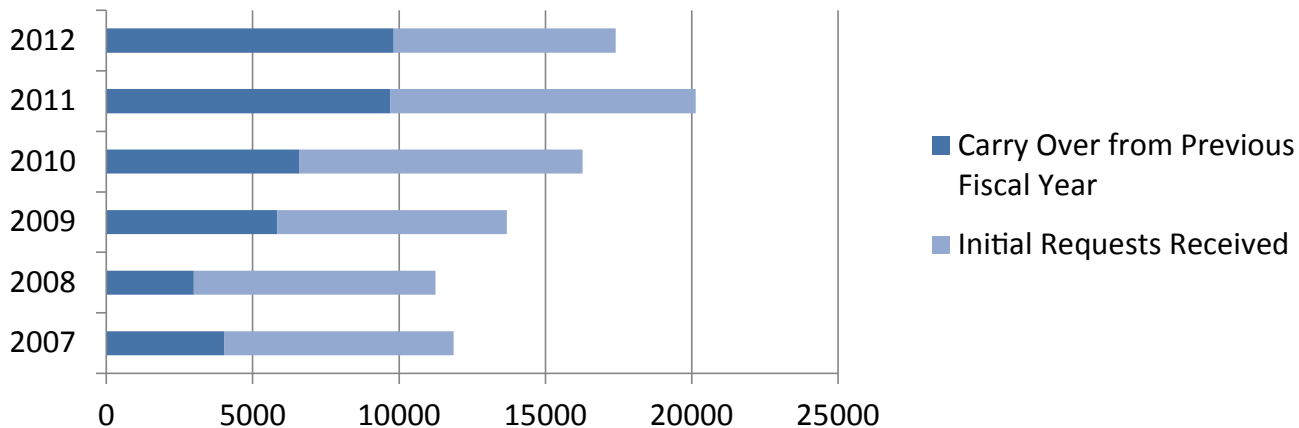


## Mandatory Declassification Review

The Mandatory Declassification Review (MDR) process under E.O. 13526 permits individuals or agencies to require specific classified national security information to be reviewed for declassification. MDR can be used in lieu of litigation of denials of requests under the FOIA, and to seek declassification of presidential papers or records not subject to FOIA. In FY 2012, through this process, 58.4 percent of pages were declassified in their entirety, 23.3 percent declassified in part, and 18.3 percent were denied.

In 2012, 27 percent fewer (7,589) new MDR Requests were made than in 2011. For the first time, agencies were required to report their average response time (228 days in 2012) for closing mandatory declassification review (MDR) requests. The previously-used MDR backlog statistics were not useful in ISOO's ability to compare MDR response programs across varied sizes of agencies.

## Pending Mandatory Declassification Review Requests Continue to Rise



For the first time, agencies were required to report their average response time for closing mandatory declassification review (MDR) requests. The reporting requirement is intended to help ISOO better compare MDR response programs across varied sizes of agencies than the previously used MDR backlog statistics. In FY 2012, the average number of days to resolve an MDR response was 228.

## Mandatory Declassification Review Appeals

Agency classification positions have been overturned with some frequency in the MDR appeals process. For this reason, mandatory declassification review appeals are an increasingly popular alternative to FOIA litigation, as the courts rarely overturn agency classification positions. The number of pages reviewed has increased every year of the last three: by 32% between 2010 and 2011, and by 147% (to 10,920) in 2012.

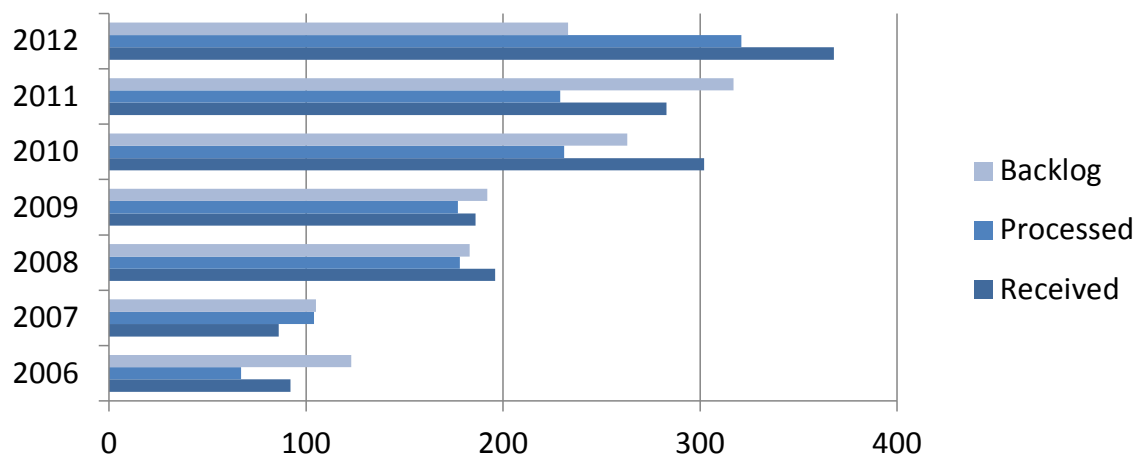
In 2012, Agencies reviewed 147% more pages (10,920) under the MDR appeals process than in 2011 (4,405), after increasing by 32% between 2010 and 2011. Through MDR appeals review, agencies declassified 60.6% in their entirety or in part, and denied declassification 39.4% of pages.

From 2006 to 2011, the backlog of appeals grew 160 percent, to 317. In 2012, agencies reduced the backlog to 233. In 2012, agencies received 368 appeals and processed 321.

“Agencies are classifying too much information, and when their peers in other agencies look at it, they say, ‘You know, that doesn’t really need to be classified.’”

**VIDEO:** Steven Aftergood discusses the benefits of MDR appeals review.

## Reported Backlog of MDR Appeals at Agencies Drops



## Interagency Security Classification Appeals Panel (ISCAP)

A requester may appeal, directly to the ISCAP, any final\* agency MDR appeal decision to deny information. The ISCAP exercises presidential discretion in its decisions and it serves as the highest appellate authority for MDR appeals.

In 2012, the ISCAP reviewed 35 MDR appeals (a total of 163 documents). The Panel declassified additional information in 150 documents, and affirmed classification decisions in 13 documents. According to ISOO, the Panel has declassified additional information in 68 percent of its reviewed documents since May 1996. In September 2012, the ISCAP staff launched a new website<sup>42</sup> to publish electronic versions of the documents declassified by the panel for public use.

Section 3.3 (h) of Executive Order 13526 required significant revisions to agency exemptions from automatic declassification, which agencies frequently made in their revisions to their declassification guides. ISCAP has the authority to approve, deny, or amend the exemptions from Automatic Declassification sought by agencies and in 2012, began the process for 23 guides. ISCAP required agency declassification offices to specifically identify information to be exempted from automatic declassification at the end of 25 years, and cases that would exempt information from automatic declassification for 50 to 75 years. The Panel approved five guides in FY 2012 and the rest in FY 2013.

## Reclassification

In April 2006, NARA began reporting quarterly<sup>43</sup> on withdrawals of previously declassified records. The reports provide information—including number of records and number of textual pages withdrawn—about records formally withdrawn in accordance with ISOO’s April 2006 “Interim Guidelines Governing Re-review of Previously Declassified Records at the National Archives.”<sup>44</sup> Through 2007, seven records and fifteen textual pages were formally withdrawn; there were no withdrawals in 2008; three documents were formally withdrawn in 2009, all by the Navy. Since then, no declassified records have been withdrawn.

**“The best way to approach a solution [to overclassification] is to expand the number of opportunities there are to rethink and revise classification decisions.”**

**VIDEO:** *Steven Aftergood discusses how overclassification can be addressed.*

---

\* For the ISCAP to consider an appeal, the criteria it must meet include that the appellant: has previously filed an administrative appeal with the agency; has received the final agency decision denying his or her administrative appeal, or has not received a final decision regarding the administrative appeal within 180 days of its filing, or has not received an initial decision regarding the MDR request within 365 days of its filing.

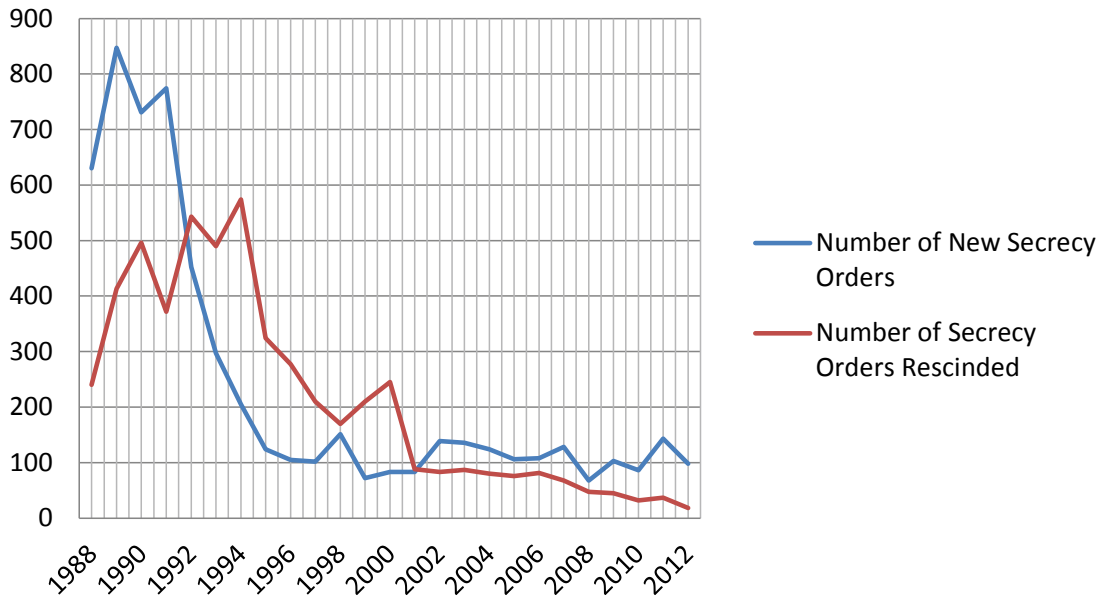
## Invention Secrecy: Secrecy Orders in Effect Continue to Climb

The federal government can impose secrecy on any new patent by issuing a “secrecy order” (35 USC 181). Although the number of new orders in 2012 (98) decreased by 31%, the number of orders rescinded also decreased, dropping 51% from 2011 (from 37 to 18). In total, 5,321 secrecy orders were in effect at the end of FY2012. Since 9/11, the number of secrecy orders in effect has continually climbed and the number of new secrecy orders per year has outstripped the number of orders rescinded.

Year	Number of New Secrecy Orders	Number of Secrecy Orders Rescinded	Total Number of Secrecy Orders in Effect
1988	630	240	5122
1989	847	413	5556
1990	731	496	5791
1991	774	372	6193
1992	452	543	6102
1993	297	490	5909
1994	205	574	5540
1995	124	324	5340
1996	105	277	5168
1997	102	210	5060
1998	151	170	5041
1999	72	210	4903
2000	83	245	4741
2001	83	88	4736
2002	139	83	4792
2003	136	87	4841
2004	124	80	4885
2005	106	76	4915
2006	108	81	4942
2007	128	68	5002
2008	68	47	5023
2009	103	45	5,081
2010	86	32	5135
2011	143	37	5241
2012	98	18	5321

Source: United States Patent and Trademark Office via Federation of American Scientists, <http://www.fas.org/sgp/othergov/invention/stats.html>; and USPTO accessed 7/24/2013

### Secrety Rescissions Continue to Decline





## Special Section: 5 Big Ideas to Kick-Start Openness

The 5 ideas discussed in this section are targeted at making noticeable changes to indicators included in our Secrecy Report. The benefits are also meant to stretch beyond simply pushing one indicator up or down, of course. The first two big ideas are intended to help reduce the number of FOIA requests sitting in queues at agencies across the government. An agency's backlog is the number of requests it has yet to process within the law's 20-day statutory time limit. Because most agencies use a "first in, first out" system (although many agencies do now offer separate tracks for "easy" and "difficult" requests), backlogs mean that there is sometimes a significant delay before an agency even begins to process a FOIA request. Smaller backlogs and less delay will help make the FOIA a more effective tool for the public to gain access to government records.

The next two ideas relate to shrinking the size of the classified universe. For decades, experts in national security have said that there is far too much material in the US classification system and argued that the vast amount of outdated or over-classified information in the system contributes to leaks.

Our final big idea is meant to ensure the public has access to secret authoritative interpretations of the law. We have seen that public access to the opinions of the FISC interpreting sections of the USA PATRIOT Act and the FISA Amendments Act has injected much-needed public oversight into the government's national security communications surveillance programs. Such public oversight is needed for all aspects of secret law.

It will take leadership and follow-through from the White House to accomplish each goal; some may be harder than others for the government to implement. Each idea, on its own, is a necessary but insufficient step towards openness and accountability.

### Big Idea 1: Start with openness.

To make the FOIA a more effective tool for requesters, the Administration should set standards for what must be released and direct agencies to make this information regularly and easily accessible (via the agencies website, as well as cross-government sites like USAspending and ethics.gov when applicable).

By setting standards for what information each agency must release, the Administration can help make sure the public has a better understanding of both what the government is doing and who is trying to influence its actions. Making information about government operations, such as contracts, visitor logs, calendars of top officials, and communications with Congress freely available online, will cut down on the number of FOIA requests needed for the information, and – as noted above – reduce backlogs and delays.

The Obama Administration has put in place several policies intended to encourage agencies to make more information available without a FOIA request being required. Attorney General Holder's [FOIA guidelines](#)<sup>45</sup> direct agencies to make proactive disclosures, and both the [Open Government Directive](#)<sup>46</sup> and the recently-released [open data policy](#)<sup>47</sup> have components intended to encourage agencies to make more information freely available.

Under all these policies, each agency is free to decide what information it should make available, how often to update the material, etc. As a result of this approach, there is a great deal of variation in the type and the quality of information currently made available. Moreover, even if an agency is releasing information, finding it on the website can be difficult for users.

On a related note, a FOIA request for a particular category of information will often yield different results from different agencies. Agencies will sometimes make different decisions about how to apply FOIA exemptions and a requester may get more or less information depending on what agency processes the request. The variation in the quantity and quality of information released makes it hard for users to compare agency programs across the government.

## Big Idea 2: Release to one is a release to all.

Any document that has been released under the FOIA should be publicly available. The government's FOIA process would be more efficient because FOIA officers would not have to process multiple similar or identical requests.

In 1986 Congress amended the FOIA to require agencies to make all “frequently requested” records available online. This change was a good first step towards reducing the number of times a FOIA officer has to process similar requests for documents. Still, though, many agencies do not have a good system for keeping track of what records are “frequently requested.” Many agencies also still default to mailing records to individual requestors, instead of putting them online.

Technological advances over the past quarter of a decade have now made it possible for the government to move much farther towards making FOIA less of a tool for one individual and a more of a lever for the public to gain access to records. With today's software and search functions, it is easier than ever for the government to put records online and for members of the public to sort through large quantities of records to find what fits their interests.

Some agencies are already beginning to take serious steps in this direction. FOIAonline, the multi-agency FOIA processing system created by the Environmental Protection Agency (EPA) gives a subscribed agency the option of making released records available in a central repository that is easy for users to search before making a request. The State Department has taken an in-house approach, adding all newly-released records to its website on a regular schedule.

## Big Idea 3: Create a self-canceling classification process.

The US should have a process that automatically declassifies without review classified information that is operational or based on a specific date or event, when that operation, date, or event passes. This would help the government streamline declassification and begin to make real progress on its backlog.

Some information that is marked as classified only needs protection for a short or a very specific period of time. The information is no longer sensitive once the event, date, or occurrence to which it pertains is over.

The current classification system (which is governed by [Executive Order 13526](#)<sup>48</sup>), includes “automatic declassification” for information after either 10 or 25 years, depending on the sensitivity of the information. Congress has prevented such “automatic declassification” from having much effect, however. The “[Kyl-Lott Amendment](#)”<sup>49</sup> to the 2009 National Defense Authorization Act requires additional review for nuclear weapons-related restricted data and formerly restricted data prior to its declassification. According to classification and declassification experts, this requirement has contributed significantly to the huge backlog of records awaiting declassification review, and hampered the efforts of the National Declassification Center (NDC).

## Big Idea 4: Reduce overclassification.

Experts have pointed out for decades the extent of and problems related to the overclassification over government information. Finally addressing the issue would help reduce the size of the classified universe. The government should kick-off this effort by creating the Security Classification Reform Steering Committee recommended by the PIDB.

As discussed later in this report, the requirement in EO 13526 that each agency with classification authority update its classification guides (a requirement called the Fundamental Classification Guidance Review) does seem to have contrib-

uted to a reduction in the number of new secrets created. A guidance review and update is not nearly enough, however, to turn the tide on the culture of secrecy at many agencies. This culture promotes both unnecessary- and over-classification. The volume of such information makes it harder to protect real secrets and degrades respect for the classification system – making leaks more likely to occur.

In the longer-term, the government must begin to change the incentive structure for classifying information and make fundamental reforms to the current system. The government should kick-off this longer-term effort by creating Security Classification Reform Steering Committee recommended by Public Interest Declassification Board’s (PIDB) November 2012 report on [Transforming Classification](#).<sup>50</sup>

**Big Idea 5: Provide public access to secret interpretations of law.**

The public must have access to legal opinions, or at least summaries of opinions, that authoritatively interpret the law. Making such secret opinions or summaries public would interject a measure of accountability into the government’s activities, especially in national security.

The public must have access to the executive and judicial interpretations of the legal rules which the government understands to control how it may operate. This access is necessary in order to have an informed debate about the government’s actions (especially those it takes under the cloak of national security). Preventing the public from understanding how the government is interpreting its obligations and restraints under the law creates a culture where no one can be held accountable for over-stepping those boundaries.

As an example, the unchecked expansion in the growth of the government’s surveillance programs is due in large measure to the absolute secrecy surrounding the FISC and how it is interpreting the law. The FISC’s opinions interpreting Section 215 of the PATRIOT Act has allowed for a much broader collection of data than most national security and civil liberties groups, and even some Members of Congress, understood the law to permit. Nor is this the first time that the government’s insistence on keeping the public in the dark about its interpretation of the law has erupted in scandal – the public was also outraged after it was revealed that the Office of Legal Counsel (OLC) had authorized the government to use interrogation techniques that meet most definitions of torture.

In light of the controversy surrounding the phone metadata collection program, President Obama announced some important steps toward letting the American public know how the Administration is interpreting provisions of the PATRIOT Act, and we have now seen that it is possible to disclose such interpretations. However, in order to make sure abuses do not continue, the Administration must commit to more transparency and openness in this and other aspects of secret law.

## Endnotes

1. Hearing of the House Judiciary Committee, Opening Statement of Mr. Robert S. Litt, General Counsel, ODNI. July 17, 2013. <http://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/894-hearing-of-the-house-judiciary-committee,-opening-statement-of-mr-robert-s-litt,-general-counsel,-odni>
2. Letter from the Honorable Reggie B. Walton to Senator Dianne Feinstein regarding FISC opinion summaries. March 27, 2013. <http://www.fas.org/irp/agency/doj/fisa/fisc-032713.pdf>
3. “Verizon Forced to Hand Over Telephone Data—Full Court Ruling.” June 5, 2013. <http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order>
4. Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act. August 9, 2013. <http://www.scribd.com/doc/159211491/Obama-administration-white-paper-on-NSA-surveillance-oversight>
5. Assistant Attorney General Letter on FISA Applications, 2009. April 30, 2010. [http://www.justice.gov/nsd/foia/foia\\_library/2009fisa-ltr.pdf](http://www.justice.gov/nsd/foia/foia_library/2009fisa-ltr.pdf)
6. Isikoff, Michael. “FBI Sharply Increases Use of Patriot Act Provision to Collect US Citizens’ Records.” June 11, 2013. [http://investigations.nbcnews.com/\\_news/2013/06/11/18887491-fbi-sharply-increases-use-of-patriot-act-provision-to-collect-us-citizens-records](http://investigations.nbcnews.com/_news/2013/06/11/18887491-fbi-sharply-increases-use-of-patriot-act-provision-to-collect-us-citizens-records)
7. Chesney, Robert. “A Tale of Two NSA Leaks.” June 10, 2013. <http://www.newrepublic.com/article/113427/nsa-spying-scandal-one-leak-more-damaging-other>
8. Statement of Todd Hinnen, Acting Assistant Attorney General for National Security, Before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security. March 9, 2011. <http://www.justice.gov/nsd/opa/pr/testimony/2011/nsd-testimony-110309.html>
9. Horwitz, Sari. “Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs.” July 17, 2013. [http://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d\\_story.html](http://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d_story.html)
10. United States Foreign Intelligence Surveillance Court. Memorandum Opinion with Exemptions. August 21, 2013. <http://www.scribd.com/doc/162016974/FISA-court-opinion-with-exemptions>
11. Lichtblau, Eric and David Johnston. “Court to Oversee U.S. Wiretapping in Terror Cases.” New York Times. January 18, 2007. <http://www.nytimes.com/2007/01/18/washington/18intel.html>
12. Ackerman, Spencer. “NSA Illegally Collected Thousands of Emails Before FISA Court Halted Program.” The Guardian. August 21, 2013. <http://www.theguardian.com/world/2013/aug/21/nsa-illegally-collected-thousands-emails-court>
13. Wyden Statement on Declassification of FISA Court Ruling on 4th Amendment Violations. August 21, 2013. <http://www.wyden.senate.gov/news/press-releases/wyden-statement-on-declassification-of-fisa-court-ruling-on-4th-amendment-violations>
14. Wakeman, Raffaella, and Ritika Singh. “The NSA Documents, Part V: The Communications with Congress.” Lawfare. August 22, 2013. <http://www.lawfareblog.com/2013/08/the-nsa-documents-part-v-the-communications-with-congress/>

15. Singh, Ritika. "Congress on the FISA Order and Data Mining Stories." Lawfare. June 7, 2013. <http://www.lawfareblog.com/2013/06/congress-on-the-fisa-order-and-data-mining-stories/>
16. Ackerman, Spencer. "Intelligence Committee Withheld Key File Before Critical NSA Vote, Amash Claims." The Guardian. August 12, 2013. <http://www.theguardian.com/world/2013/aug/12/intelligence-committee-nsa-vote-justin-amash>
17. Wallsten, Peter. "House Panel Withheld Document on NSA Surveillance Program from Members." Washington Post. August 16, 2013. [http://www.washingtonpost.com/politics/house-panel-withheld-document-on-nsa-surveillance-program-from-members/2013/08/16/944e728e-0672-11e3-9259-e2aaf5a5f84\\_story.html](http://www.washingtonpost.com/politics/house-panel-withheld-document-on-nsa-surveillance-program-from-members/2013/08/16/944e728e-0672-11e3-9259-e2aaf5a5f84_story.html)
18. Singh, Ritika. "Congress on the FISA Order and Data Mining Stories." Lawfare. June 7, 2013. <http://www.lawfareblog.com/2013/06/congress-on-the-fisa-order-and-data-mining-stories/>
19. Foreign Intelligence Surveillance Act. [http://en.wikipedia.org/wiki/Foreign\\_Intelligence\\_Surveillance\\_Act](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act)
20. Lichtblau, Eric. "In Secret, Court Vastly Broadens Powers of N.S.A." New York Times. July 6, 2013. <http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html>
21. Justice Dept Status Report Re: Releasing Secret Patriot Act Interpretation Documents. September 4, 2013. <https://www.eff.org/document/justice-department-status-report-re-releasing-secret-patriot-act-interpretation-documents>
22. "DOJ Declassifying Portions of Secret Foreign Intelligence Surveillance Court Opinions." Associated Press. September 5, 2013. <http://washington.cbslocal.com/2013/09/05/doj-declassifying-portions-of-secret-foreign-intelligence-surveillance-court-opinions/>
23. Hearing of the House Judiciary Committee, Opening Statement of Mr. Robert S. Litt, General Counsel, ODNI Wednesday, July 17, 2013. <http://www.dni.gov/index.php/newsroom/testimonies/194-congressional-testimonies-2013/894-hearing-of-the-house-judiciary-committee,-opening-statement-of-mr-robert-s-litt,-general-counsel,-odni>
24. List of Signing Statements, Issued by Barack Obama. <http://www.coherentbabble.com/signingstatements/signstateann.htm>
25. Fiscal Year 2011 Annual FOIA Report Summary <http://www.justice.gov/oip/foiapost/fy-2011-annual-report-summary.pdf>
26. Summary of Annual FOIA Reports; 2012 statistics accessed 7/22/2013. <HTTP://WWW.JUSTICE.GOV/OIP/DOCS/FY2012-ANNUAL-REPORT-SUMMARY.PDF>
27. Department of Justice FOIA 2009 Handbook [http://www.justice.gov/oip/foia\\_guide09/exemption5.pdf](http://www.justice.gov/oip/foia_guide09/exemption5.pdf)
28. Presidential Memorandum -Managing Government Records. November 28, 2011. <http://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records>
29. Managing Government Records Directive, <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>
30. Records Management Self-Assessment (RMSA) 2012 <http://www.archives.gov/records-mgmt/resources/self-assess->

ment.html

31. Office of Special Counsel FY 2014 Congressional Budget Justification. <http://www.osc.gov/documents/reports/FY%202014%20Congressional%20Budget%20Justification.pdf>
32. Memorandum Re: Federal Circuit Whistleblower Decisions Since Passage of 1994 Amendments [http://www.openthe-government.org/sites/default/files/Federal\\_Circuit\\_digest%208%2016%202013.pdf](http://www.openthe-government.org/sites/default/files/Federal_Circuit_digest%208%2016%202013.pdf)
33. Jewel v. NSA, <https://www.eff.org/cases/jewel>
34. Department of Justice 2009 policy, <http://www.justice.gov/opa/pr/2009/September/09-ag-1013.html>
35. Erwin, Marshall C. and Amy Belasco. "Intelligence Spending and Appropriations: Issues for Congress." Congressional Research Service. September 5, 2013. <http://www.fas.org/sgp/crs/intel/R42061.pdf>
36. DNI Releases Updated Budget Figure for FY 2014 Appropriations Requested for the National Intelligence Program. June 27, 2013. <http://www.fas.org/irp/news/2013/06/nip-2014.pdf>
37. DOD Releases Revised Military Intelligence Program Request for Fiscal Year 2014. <http://www.fas.org/irp/news/2013/06/mip-2014.html>
38. Aftergood, Steven. "Number of Security Cleared Personnel Grew in 2012." Secrecy News. April 15, 2013. [http://blogs.fas.org/secrecy/2013/04/2012\\_clearances/](http://blogs.fas.org/secrecy/2013/04/2012_clearances/)
39. Executive Order 13526- Classified National Security Information, December 29, 2009. <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>
40. ISOO 2012 Annual Report to the President <http://www.archives.gov/isoo/reports/2012-annual-cost-report.pdf>
41. Bi-Annual Report on Operations of the National Declassification Center: Reporting Period July 1, 2013- December 31, 2012. [http://www.fas.org/blog/secrecy/2012/02/cia\\_mdr.html](http://www.fas.org/blog/secrecy/2012/02/cia_mdr.html)
42. Interagency Security Classification Appeals Panel (ISCAP) Released Documents <http://www.archives.gov/declassification/iscap/decision-search.html>
43. Quarterly Report of Withdrawals of Previously Declassified Records <http://www.archives.gov/about/plans-reports/withdrawn/>
44. Interim Guidelines Governing Re-review of Previously Declassified Records at the National Archives <http://www.archives.gov/isoo/reports/2006-audit-report-attach-2.pdf>
45. FOIA Memo for the Heads of Executive Departments and Agencies. March 19, 2009. <http://www.justice.gov/ag/foia-memo-march2009.pdf>
46. OMB Open Government Directive. December 8, 2009. [http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda\\_2010/m10-06.pdf](http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf)
47. Open Data Policy-Managing Information as an Asset. May 9, 2013. <http://www.whitehouse.gov/sites/default/files/>

omb/memoranda/2013/m-13-13.pdf

48. Executive Order 13526- Classified National Security Information. December 29, 2009. <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>

49. Sec. 3161. Protection against inadvertent release of restricted data and formerly restricted data. September 22, 1998. <http://www.fas.org/sgp/congress/hr3616am.html>

50. “Transforming Classification: 2012 Report to the President.” Public Interest Declassification Board. November 2012. <http://www.archives.gov/declassification/pidb/recommendations/transforming-classification.html>