S. Hrg. 113–367

STRENGTHENING GOVERNMENT OVERSIGHT: EXAMINING THE ROLES AND EFFECTIVENESS OF OVERSIGHT POSITIONS WITHIN THE FEDERAL WORKFORCE

HEARING

BEFORE THE

SUBCOMMITTEE ON THE EFFICIENCY AND EFFECTIVENESS OF FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 19, 2013

Available via the World Wide Web: http://www.fdsys.gov

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

86–637 PDF WASHINGTON : 2014

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEIKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
KEITH B. ASHDOWN, *Minority Staff Director*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN CORCORAN, *Hearing Clerk*

SUBCOMMITTEE ON THE EFFICIENCY AND EFFECTIVENESS OF FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE

JON TESTER, Montana, *Chairman*

MARK L. PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming

TONY MCCLAIN, *Majority Staff Director*
BRENT BOMBACH, *Minority Staff Director*
KELSEY STROUD, *Chief Clerk*

CONTENTS

STRENGTHENING GOVERNMENT OVERSIGHT: EXAMINING THE ROLES AND EFFECTIVENESS OF OVERSIGHT POSITIONS WITHIN THE FEDERAL WORKFORCE

TUESDAY, NOVEMBER 19, 2013

U.S. SENATE,
SUBCOMMITTEE ON THE EFFICIENCY AND EFFECTIVENESS OF FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE,
OF THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m., in room 342, Dirksen Senate Office Building, Hon. Jon Tester, Chairman of the Subcommittee, presiding.

Present: Senators Tester, Portman and Johnson.

OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. I will call to order this hearing on the Subcommittee on Efficiency and Effectiveness of Federal Programs and the Federal Workforce.

This afternoon's hearing is titled Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions within the Federal Workforce.

I want to thank Senator Portman, who will be here shortly, for his ongoing engagement and leadership on this Subcommittee, and we look forward to continuing our partnership as we move forward the hearings that are in front of us.

I want to thank our witnesses for joining us today and for their ongoing work that brings greater oversight, accountability and transparency to the Federal Government.

I can tell you that folks back in Montana are a bit skeptical about the way things work in Washington. I hear about it every weekend when I go home.

So they see news coverage of lavish retreats and of conferences hosted by government agencies on the taxpayer dime. They read about millions wasted on construction contracts in Afghanistan that are not needed or cannot be sustained. They hear about the latest infringement of their privacy by government programs carried out in the name of national security.

And so I do not blame them for being a bit wary of what is going on here in Washington, DC. In fact, I often feel the same way.

Today, over two million men and women make up our Federal workforce. They administer programs and initiatives that touch upon every aspect of our lives.

And we know that good oversight comes with the executive and legislative branches working together. We need partnerships within the executive branch. Without independent voices of oversight within the Federal agencies, including the folks that are here today, we have no hope for accountability or transparency, and we certainly have no hope of maintaining the public trust in our government.

As I told the Council of Inspectors General earlier this year, they, along with our privacy officers, comptrollers and oversight officials, have some of the toughest jobs in government.

I know that when you call an agency head or division chief, they do not often sprint to the phone to pick it up, and you frequently have to fight for access that you need to do your jobs. And I get that.

It is critical that you let us know when impediments prevent you from performing effectively your roles of oversight, whether it is a lack of authority or resources.

Earlier this year, in the wake of Edward Snowden leaks, the Subcommittee held a hearing on security clearance reforms. At that meeting, we learned that the Inspector General (IG) of the Office of Personnel Management (OPM) was precluded from using funds from the OPM's revolving fund for audits and oversight. This is a $2 billion fund that finances background investigations as well as other OPM programs such as human resource solutions and USAJobs.

Because the OPM IG is unable to access these funds, rigorous oversight is not being performed and a financial audit on the fund in its entirety has never happened. So I, along with Senators Portman and McCaskill, Senators Johnson and Coburn, subsequently introduced a bill to provide the OPM IG's office with the access that it needed to those funds.

The SCORE Act has now passed the Senate, and we are closer to seeing the level of oversight of this fund that should have been performed a long time ago. But it is good news where we are at today for taxpayers, and I think it is good news for our national security. We need our House colleagues to move forward on the SCORE Act.

The point is that we can be productive partners with the oversight workforce to effect change. All that is required is an open and frank line of communication. We are here to help, but we often need folks like you to serve as our eyes and our ears within the agencies. Whether it is reining in wasteful spending, holding individuals and agencies accountable for wrongdoing, shining a light on government operations or protecting the privacy rights of law-abiding Americans, we want to empower you and your efforts.

Today, with this hearing, we hope to examine the various roles currently played by our Federal oversight workforce, to explore some of the challenges that you confront and to identify ways to overcome those challenges. And I look forward to the discussion today.

With that, I want to welcome Senator Portman, Ranking Member of this Committee, and turn it over to him for his opening statement.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you, Mr. Chairman. I appreciate it.

Thank you all for being here today.

As you know, this Committee, and specifically this Subcommittee, relies on you, and we love to drag you up here and have you join other expert witnesses to tell us what is really going on in your agencies.

We are concerned, frankly, with the vacancies, and that is one reason we wanted to have this hearing today. We think Inspectors General and their oversight offices are key as the watchdogs of the Federal Government.

We are looking at fraud and abuse, efficiency and effectiveness even outside of fraud and abuse. We like to get your input on pending legislation and regulations. And we have all got a big task. So we need the independent oversight professionals like yourselves.

On the vacancy issue, since early 2009, we have had a real issue here. At its height of this problem of lack of IGs, in the 12 cabinet departments and major Federal agencies, we were without a permanent IG. That was the worst that it has been as far as we can tell in the history of IGs.

In fact, at the State Department, as some of you know, we had a vacancy there that went over 1,400 days, not having a permanent IG at the State Department really for the whole first term.

Such vacancies leave these offices without proper leadership, and as a result, we have seen allegations of political influence and suppression of the IG office at the Department of State, and allegations of abuse of power and misconduct at the Homeland Security IG Office.

So we also want to be sure that we can have trust in our oversight professionals because when you cannot there is a serious breakdown in the management of any organization, let alone such large and important Federal agencies.

So, with the current financial status of the Federal Government and our now $17 trillion debt, we certainly owe it to our constituents to ensure their tax dollars are being spent in the right way—the most efficient and effective way possible. And it is the oversight workforce, you all, who are on the front lines to ensure that happens. So we want to continue to find ways to support and empower IGs and the oversight community.

So thank you, Mr. Chairman, for holding this hearing today. I look forward to the testimony as we move forward together to achieve that goal.

Senator TESTER. Thank you, Senator Portman. I appreciate your words.

Senator Johnson, do you have an opening statement?

Senator JOHNSON. No.

Senator TESTER. OK. Well, what I will do is, first of all, I want to welcome you all once again to the hearing today. We are very fortunate to have such a great panel of witnesses. I will introduce

you all right now, and then we will start with Peg and just go right down the line.

Peggy Gustafson is the Inspector General of the United States Small Business Administration (SBA). As Inspector General of SBA, she heads up the audit and investigative programs that seek to identify fraud, waste, abuse and mismanagement in programs at SBA.

She also is the head of the Legislation Committee for the Council of Inspectors General on Integrity and Efficiency (CIGIE). CIGIE members include 72 IGs from the executive and legislative branches of government as well as 6 senior Administration officials with related portfolios and responsibilities.

Welcome, Peg.

We have Michael Horowitz, who is the Inspector General for the United States Department of Justice (DOJ). He oversees an oversight workforce of approximately 450 special agents, auditors, inspectors, attorneys and support staff. Their mission is to detect and deter waste, fraud and abuse and misconduct in the Department of Justice programs and personnel, and to promote economy and efficiency in the Department's operations.

Welcome, Michael.

Carolyn Lerner is the head of the Office of Special Counsel (OSC), an independent investigative and prosecutorial Federal agency. Among other missions, the OSC protects the merit system for 2.1 million civilian Federal employees, provides a channel through which whistleblowers can report waste, fraud and abuse, and enforces the Uniform Services Employment and Reemployment Rights Act (USERRA), which upholds the employment rights of our Service members.

Carolyn, thank you for being here.

Karen Neuman was recently named as Chief Privacy and Freedom of Information Act Officer for the Department of Homeland Security (DHS). She leads the first statutorily mandated privacy office in any Federal agency. That office is tasked with protecting Americans by embedding and enforcing privacy protections and transparency in all DHS activities.

Once again, welcome, Karen.

Wendy Ginsberg is an analyst in American National Government of the Congressional Research Service (CRS). She received her Ph.D. from the University of Pennsylvania in 2011. We are very happy to have her historical perspective on all things oversight today.

I want to welcome you, Wendy.

And thank you all for being with us today.

It is custom to swear in all witnesses who appear before this Subcommittee. So, if you do not mind, please stand and repeat after me.

Do you swear that the testimony you are about to give before this Subcommittee will be the truth, the whole truth and nothing but the truth; so help you, God?

Ms. GUSTAFSON. I do.

Mr. HOROWITZ. I do.

Ms. LERNER. I do.

Ms. NEUMAN. I do.

Ms. GINSBERG. I do.

Senator TESTER. Let the record reflect that the witnesses answered in the affirmative.

We will start with you, Peg. You can start with your presentation.

TESTIMONY OF THE HON. PEGGY E. GUSTAFSON,[1] INSPECTOR GENERAL, SMALL BUSINESS ADMINISTRATION, AND CHAIR, LEGISLATION COMMITTEE, COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY (CIGIE)

Ms. GUSTAFSON. Good afternoon, Chairman Tester, Ranking Member Portman and Members of the Committee. On behalf of the Chair of the Council of the Inspectors General on Integrity and Efficiency, I am honored to represent the Federal Inspector General community this afternoon to discuss our work and recent accomplishments as well as some of the challenges we face in carrying out our oversight duties.

I want to begin by thanking the Subcommittee on behalf of the IG community for your continuing support of our mission and your interest in our work. The support of the Subcommittee has been longstanding and bipartisan, and we very much appreciate that.

I am pleased to report that the Inspector General Reform Act of 2008 is working as intended. CIGIE serves a leadership role and is the core of the IG community. Together, the work of the IG community has resulted in significant improvements to the economy and efficiency of programs governmentwide, with potential savings totaling approximately $46.3 billion in fiscal year (FY) 2012. With the IG community's aggregate budget of approximately $2.7 billion in that year, these potential savings represent about a $17 return on every dollar invested in the IG community.

Notwithstanding these results, IGs do face certain challenges as they work to improve the efficiency and effectiveness of government programs. Our principal challenges pertain to independence concerns and timely access to information that we need to perform our duties. In recent years, we have been advocating for some additional tools to alleviate these challenges.

For example, CIGIE feels strongly that Offices of Inspector General (OIG) should be exempted from the Computer Matching and Privacy Protection Act relative to using electronic means to identify those who improperly receive Federal assistance and payments and subsequently, seek removal of those persons from the program after verification of this information and due process is applied. This would improve program efficiency throughout the government.

Similarly, CIGIE has recommended that the Paperwork Reduction Act (PRA) be amended to exempt Federal IG Offices. The PRA requires that information collection, such as surveys that we may want to do of a certain community, be subject to approval from a senior official of the agency, not the IG Office but a Federal agency, and also from the Office of Management and Budget (OMB). While changes have been made to the PRA to exempt independent regulatory agencies and the Government Accountability Office (GAO) remains exempt from the PRA, all laws have been silent as to the

[1] The prepared statement of Ms. Gustafson appears in the Appendix on page 35.

application of the PRA to IGs. We believe that if these exemptions could be provided to IG Offices, it would enhance our independence and remove lengthy processes that are hampering our ability to do our job.

In the last few years, the IG community has been hit especially hard by the uncertainty in the budget process and cuts to operating budgets. Offices of Inspector General, by nature, are comprised principally of personnel, and their budgets are dedicated to funding the same. A recent survey of the IG community by the Association of Government Accountants has found that more than two-thirds of IGs interviewed identified budget resources as a top challenge. Many of our offices have undertaken hiring restrictions, hiring freezes and limited new investments in order to operate under the current budget levels. To highlight this finding, right now in my office, we are suffering an approximately 17 percent vacancy rate in positions that we simply have not been able to fill in order to maintain the current spending levels.

I am grateful that IGs across the government have a voice through CIGIE and have access to training and other resources that have been provided to them in the IG Reform Act. In conjunction with that, our training academy has trained last year 1,677 IG employees, representing a 17 percent increase of students from our previous year.

In addition, and in accordance with CIGIE's primary mission, over the past several years, the IG community has identified and addressed a number of issues that transcend individual agencies through cross-cutting projects, as talked about and mentioned and suggested in the IG Reform Act.

For example, CIGIE has issued reports on such topics as cybersecurity, the use of suspension and debarment throughout the Federal Government, the use of new media, the effectiveness of the CFO Act, disaster preparedness programs in the various agencies, international trade and competitiveness, as well as things like our hotline operations and whistleblower protections. All of these reports are public and available on CIGIE's Web site.

In conclusion, I would just like again to emphasize that I am very proud and pleased to represent the IG community. I am very happy to be back in this hearing room, where I have spent a lot of time in my previous iteration. And I am grateful for the chance to take your questions.

Thank you.

Senator TESTER. Well, thank you, Peg. And the fact that your testimony ran 20 seconds short of 5 minutes shows that you are not new to this party; you have been here before.

And we appreciate it because I forgot to tell you up front that you have 5 minutes for your oral statement and your entire statement will be put in the record.

With that, thank you.

Michael, you are up to bat.

TESTIMONY OF THE HON. MICHAEL E. HOROWITZ,[1] INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE

Mr. HOROWITZ. Thank you, Chairman Tester, Senator Portman, Members of the Subcommittee. Thank you for inviting me to testify at today's hearing.

The need for strong and effective independent oversight over agency operations has never been more important. I am pleased to highlight for you examples of our oversight work as well as some obstacles we face in conducting that independent oversight.

During my 18 months as Inspector General of the Department of Justice, our office has issued reports ranging from our review of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATFs), Operations Fast and Furious and Wide Receiver, to our interim report on the Department's handling of known or suspected terrorists in the Witness Security (WITSEC) Program to our audit of ATF's income-generating undercover operations. We issued 90 audit reports in this past year which will help make the Department's operations more effective and efficient.

Our Investigations Division had dozens of arrests and convictions during that same period of time and investigated allegations that resulted in more than 250 administrative actions against Department employees.

Additionally, we conducted extensive oversight of the Department's use of its national security-related authorities. For example, we issued reports on the Federal Bureau of Investigation's (FBI) activities under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act and the FBI's Foreign Terrorist Tracking Task Force's sharing of information. And we expect to issue, in the near future, reviews on the FBI's use of National Security Letters (NSL), Section 215 Orders and Pen Register and Trap-and-Trace Authorities under FISA, as well as on the management of terrorist watch list nominations.

The oversight we conduct routinely produces measurable benefits for taxpayers. Over the past 10 fiscal years, we identified over $900 million in questioned costs, far more than our budget during that same period. In addition, we identified nearly $250 million in taxpayer funds that could have been put to better use, and our criminal and administrative actions resulted in more than $118 million in various recoveries.

And I am particularly proud of having instituted our office's first ever whistleblower ombudsperson program. I have seen firsthand the important role whistleblowers play in advancing our mission, and whistleblowers should never suffer reprisal for coming forward with what they reasonably believe to be evidence of waste, fraud, abuse and misconduct.

Let me turn now to some of the challenges we faced in conducting our oversight.

As we all know, these are difficult budgetary times across the government, including for Inspectors General, and sequestration is having a real impact on our office. The substantial budget reduction for our office in fiscal year 2013, combined with the uncertain budget situation for fiscal year 2014, has caused me to lower our

[1] The prepared statement of Mr. Horowitz appears in the Appendix on page 38.

staffing levels by approximately 8 percent, or 40 full time equivalent (FTEs), since I took office in April 2012. Further reductions in our staffing will inevitably require us to reduce the number of audits, investigations and reviews that we conduct, and it may also impact how we proceed with those that we do conduct. It may impact on the scope of those reviews and cause us to overemphasize the importance of budgetary decisions in choosing those audits, investigations and reviews.

However, let me say, despite those financial issues, I am confident the dedicated professionals in our office and in all OIGs will continue to provide the extraordinary service to the American public that they have demonstrated over the years.

I want to address the issue mentioned earlier, which is access to documents. For any OIG to have the ability to conduct effective oversight, it must have complete and timely access to all records in the agency's possession. This principle was codified by Congress in Section 6(a) of the Inspector General Act.

Most of our audits and reviews are conducted with full and complete cooperation. However, there have been occasions when our office has had access issues due to the Department's views regarding access and being limited by other laws.

Such issues arose in Fast and Furious and our current review of the Department's use of material witness warrants in connection with grand jury and wiretap records. In both of those instances, the Attorney General (AG) and Deputy Attorney General came forward and provided us with written permission to gain access to those records, and they both indicated they will continue to do that in the future. But the issue is that having an Inspector General have to go to its agency head to get approval and to get that permission—that impairs our independence, and it conflicts with the core principles, in our view, of the Inspector General Act.

And I understand from speaking with several other Inspectors General that they have had similar issues.

I believe the view of my colleagues in the Inspector General community is straightforward and follows from what is explicitly stated in the IG Act. An Inspector General should be given prompt access to all relevant documents within the possession of its agency.

Finally, I have outlined another limitation in my testimony, which is unique to my OIG, which is we do not have oversight authority over all misconduct in our agency. We have authority over non-attorneys, but we do not have authority over attorneys whose misconduct is alleged to have occurred in the course of their litigating authority. That is an anomaly of history, as I outline in my testimony. It is something we believe should be corrected. Other IGs across the Federal IG community have that authority, and we think we should have that authority as well.

Thank you, Mr. Chairman.

Senator TESTER. Thank you, Michael. Appreciate your testimony.

Carolyn, you are up.

TESTIMONY OF THE HON. CAROLYN N. LERNER,[1] SPECIAL COUNSEL, U.S. OFFICE OF SPECIAL COUNSEL

Ms. LERNER. Chairman Tester, Ranking Member Portman, Senator Johnson, Members of the Committee, thank you for the opportunity to testify.

The Office of Special Counsel, protects the merit system for over 2.1 million Federal civilian employees. We have a very broad mission. We provide a safe and secure channel for whistleblowers to report government wrongdoing. We protect employees from prohibited personnel practices, especially retaliation for whistleblowing. We enforce the Hatch Act. And we protect the employment rights of veterans and Service members employed by the Federal Government.

We do all this with 110 employees and the smallest budget of any Federal law enforcement agency. While our staff is more efficient and effective than at any point in OSC's 35-year history, our capacity for improving government is limited by serious resource challenges.

OSC's caseload is historically high. It has nearly doubled in the last 5 years. But our staffing is at the same level as it was 10 years ago. And, despite the increases in our workload, OSC's already flat budget took a dramatic hit with sequestration. The combination of high caseloads and a shrinking budget threatens OSC's oversight potential.

The good news is that Congress and the Administration recognized that the status quo is not sustainable. The President's Fiscal Year 2014 budget request for OSC provides for an increase of approximately $1.7 million, which both the House and Senate Appropriations Committees have approved. I am very hopeful that the final spending bills for 2014 will include this total.

With that overview, I want to provide a little bit more detail on OSC's recent successes.

The last 2 years have been a record-setting period. By nearly every statistical measure, OSC achieved the most positive results in its history, and these successes result in greater confidence in OSC. However, such confidence can be a double-edged sword as it directly correlates to our skyrocketing caseload.

Our increased efficiency helps us manage this growing caseload, and it also translates into real savings. In the last 5 years, OSC's cost to resolve a case dropped by 40 percent. So we are doing a lot more efficiently.

And we are getting more favorable actions for whistleblowers, such as back pay or reinstatement for victims of retaliation, as well as disciplinary actions against supervisors who retaliated or engaged in other prohibited conduct. In 2012, our staff achieved a remarkable 89 percent increase in favorable actions from the prior fiscal year, far surpassing the number achieved in any previous year in history, and the total number of favorable actions rose again last year.

But the numbers do not tell the whole story. Our efforts often stop the immediate problem and spark systemic reforms that pre-

[1] The prepared statement of Ms. Lerner appears in the Appendix on page 45.

vent wasteful, inefficient or unsafe practices, and we save the government money.

For example, 2 weeks ago, we issued a report detailing serious overtime abuse by the Department of Homeland Security, costing the government tens of millions of dollars annually. Thanks to this Subcommittee and others, reform is already underway, and I look forward to returning on December 10 to testify a little bit more about our report in that case.

Also, in the past year, OSC worked with whistleblowers at the VA Medical Center (VAMC) in Jackson, Mississippi. Physicians and other employees raised concerns about unlawful prescriptions and unsterile medical equipment among a range of other issues affecting patient safety. OSC's efforts in that case have resulted in greater oversight by the Administration and Congress.

In the last 2 years, OSC also successfully carried out its expanded role to protect the rights of veterans and Service members under the Uniformed Services Employment and Reemployment Rights Act. We have always prosecuted USERRA cases before the Merit System's Protection Board (MSPB), but under a 3-year pilot project mandated by Congress, OSC is also investigating half of all Federal sector USERRA claims while the Department of Labor (DOL) continues to investigate the other half.

We resolve many of our cases through alternative dispute resolution—a low cost and highly effective approach. It is particularly effective in USERRA cases, where we have a 100 percent success rate.

OSC is also implementing the Whistleblower Protection Enhancement Act (WPEA) which became law in 2012. We are the primary agency responsible for enforcing this law, and we are seeing a significant increase in claims. In the first quarter after the Act was passed, we had the highest number of filings in our entire history.

The Congressional Budget Office (CBO) conservatively estimated that we would need about $1 million more each year to successfully implement the WPEA. However, under sequestration, our resources have actually been cut by about a million dollars since the enactment of the WPEA.

Investing in OSC is one of the most cost effective methods of promoting good government and preventing violations of the merit system laws. Whether we are enforcing the Hatch Act, USERRA, the Whistleblower Protection Act or the laws protecting employees from prohibited personnel practices, OSC provides a high return to the Federal Government and the public.

I thank you for the opportunity to testify today, and I look forward to hearing your questions.

Senator TESTER. Thank you, Carolyn. Appreciate your testimony.

Karen Neuman, you are up.

TESTIMONY OF KAREN NEUMAN,[1] CHIEF PRIVACY AND FREEDOM OF INFORMATION ACT OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. NEUMAN. Thank you.

Good afternoon, Chairman Tester, Ranking Member Portman, Senator Johnson and Members of the Subcommittee. I am very pleased to be here today to discuss the DHS Privacy Office and our oversight responsibilities.

I joined the Department of Homeland Security as the Chief Privacy Officer just under 1 month ago. In this short time, I have experienced firsthand the broad responsibilities borne by this small, but critically important, office and the commitment of the staff to ensuring that privacy is embedded throughout the Department's programs. Our holistic approach to privacy protection reflects our statutory policy, compliance and oversight responsibilities.

I would like to address some of the specific questions you raised in your invitation to testify today.

You asked about privacy and transparency. In addition to my duties as Chief Privacy Officer, I am also the Department's Chief FOIA Officer, and I understand the importance of transparency in that respect.

Transparency is also central to our mission to protect privacy. It is the first of the Fair Information Practice Principles that guide the work of my office. Transparency lets the public understand what information we collect from them, how we use it across our vast mission set, how long we will keep it and who we might share it with.

To promote transparency, the Privacy Office has published hundreds of privacy impact assessments (PIAs), and system of records notices (SORNs), on our public Web site. Our PIAs are often the fullest description to the public of how DHS activities and programs collect and use information and the specific measures we take to provide a high level of privacy protection.

The Privacy Office is able to provide this level of protection because we operationalize privacy throughout the Department. Our privacy and compliance teams work with DHS programs and system owners at the earliest stage of development, planning and implementation to identify potential privacy risks.

For example, the compliance team may identify risks associated with a particular program and help craft corrective measures whereas the policy team identifies complex or novel privacy issues that may have department-wide implications which can be addressed through DHS-wide directives or policies.

I think from what I have seen in the short time I have been here that our efforts to operationalize privacy have been very effective.

You also asked about oversight. The Privacy Office implements its oversight authority through a new oversight team within the office that was established by my predecessor. The team uses a suite of tools for reviewing the Department's use of personally identifiable information (PII), each with the goal of improving data stewardship. These tools include collaborative privacy compliance re-

[1] The prepared statement of Ms. Neuman appears in the Appendix on page 51.

views, privacy investigations, privacy incident response and privacy complaint handling and redress.

The oversight team has forged close working relationships with other oversight authorities, including the DHS Office of Inspector General, GAO, OMB and the Privacy and Civil Liberties Oversight Board (PCLOB).

I believe this layered approach has been extremely effective at avoiding duplication of effort while leveraging the highly specialized expertise of the Privacy Office.

You also asked how well our incident response program is functioning. We have a great working relationship with the component privacy offices and security staff and the DHS Security Operations Center, who are the privacy incident first responders.

The Privacy Office provides guidance and oversees the process to ensure that breaches or other incidents are properly mitigated and remediated, and if we have questions about the adequacy of the response, we may reach out to the components involved to ascertain facts and work toward an effective resolution.

DHS policy requires staff to report known or suspected privacy incidents, and reporting has consistently improved over the years as incident response training has intensified. I believe this program is working well.

I would like to share a few examples with you where we have integrated privacy policy compliance and oversight to provide clear benchmarks for evaluating adherence to DHS privacy policy. These areas include our review of some of the Department's screening rules, Privacy Office clearance of certain intelligence products, and our review and evaluation of major systems' privacy compliance in preparation for the Department's annual budget submission.

Finally, you asked about the office's role in the budget and policy process. My office reviews and evaluates major systems' privacy compliance in preparation for the Department's annual budget submission. More broadly, the Privacy Office has meaningful input into this submission in order to carry out all of our functions.

Budget reductions and sequestration have resulted in an inability to backfill key positions that have been vacant. That we are meeting our obligations really speaks to the commitment and professionalism of the Privacy Office staff. Maintaining and strengthening our workforce is a key priority of mine to ensure that our mission does not suffer.

In closing, I would like to thank you again for your invitation to address you this afternoon, and I look forward to taking your questions.

Senator TESTER. Thank you very much, Karen, for your comments.

Wendy Ginsberg.

TESTIMONY OF WENDY GINSBERG,[1] PH.D., LIBRARY OF CONGRESS, CONGRESSIONAL RESEARCH SERVICE

Ms. GINSBERG. Chairman Tester, Ranking Member Portman, Senator Johnson, thank you for the opportunity to testify before you today on technology's effects on Federal oversight.

[1] The prepared statement of Ms. Ginsberg appears in the Appendix on page 59.

In 1885, Woodrow Wilson said that Congress should use every means to oversee the executive branch. Otherwise, he argued the country would remain in embarrassing, crippling ignorance of the very affairs which it is most important it should understand and direct.

In this testimony, I make three broad points. First, evolving technologies can assist in oversight. Second, the use of these technologies has advantages and disadvantages. And, finally, technology must be thoughtfully and carefully implemented if it is to assist Federal oversight.

To my first point, that technology can assist oversight, it is important to first note that oversight lacks a precise definition. In fact, it is not mentioned in the Constitution. Yet, oversight is an implicit obligation of Congress.

It can be performed in various ways to meet many objectives. Congress has created a variety of tools to assist its oversight function. Among these tools are hearings, reporting requirements, general management laws and the creation of an oversight workforce, which includes institutions like the Government Accountability Office and the 72 offices of Inspectors General.

Additionally, Congress and the President have employed new and evolving technologies to increase information access and, arguably, have facilitated greater public participation in the oversight process.

One example of such an initiative is the Obama Administration's Open Government Initiative, which employs four core strategies: first, publish government information online; second, improve the quality of government information; third, create and institutionalize a culture of open government; and fourth, create an enabling policy framework for open government.

Private sector reviews of the initiative suggest that agencies varied in their open government achievements. Perhaps to address some of these criticisms, the Administration began promoting what it called smart disclosure, which requires agencies to release complex information and data in standardized, machine-readable formats that enable consumers to make informed decisions.

Another transparency-related oversight mechanism was the establishment of the Web site, Recovery.gov. It was created in compliance with the American Recovery and Reinvestment Act of 2009. The public-facing Web site includes information about the Recovery Act and the distribution of Federal funding related to the Act. It, arguably, allowed taxpayers to be in a better position to hold their government accountable.

Similar technology was used to create other public-facing Web sites, including USASpending.gov, Data.gov and Performance.gov.

Additionally, the 72 offices of Inspectors General have employed technology in a variety of ways to assist Federal oversight. The variance in department and agency missions, however, prompts variety in how Inspectors General conduct oversight and, therefore, disparate adoption of technologies within the Inspector General community.

A 2011 survey conducted by the Council of Inspectors General on Integrity and Efficiency found that only 26 of more than 70 Inspectors General reported using any form of new media.

Next, to my second point that use of technology has advantages and disadvantages, employing technology and new media can assist Federal oversight but can complicate information security, privacy, legal oversight and records collection. Continued use of large databases and new media may require investments in training, equipment, personnel and other resources. Additionally, existing statutes, regulations or policies may need to be revisited to determine whether they encumber IGs, the public or other entities from effectively using online tools and data to assist oversight.

Technology can assist in government oversight. It can provide new information and allow overseers to use data in innovative ways.

Technology and use of new media can assist in investigations and facilitate public input on agency actions. Providing interested stakeholders access to information can allow them to track where Federal dollars are spent, can provide context on the methodology used to rate the most effective child safety seat or can provide data on the spread of the flu virus. This access may help uncover fraud, improve safety or even save lives.

And my final point, agencies must determine which technologies to employ based on their mission and their resources. Technology must be thoughtfully implemented, and sensitive data and information must remain protected.

Mr. Chairman, this concludes my opening statement. Thank you for the opportunity to testify, and I look forward to your questions.

Senator TESTER. Thank you, Wendy.

And I want to thank everybody who testified here.

We will put 7 minutes on the clock for questions, and we will just kind of go down the line.

Peg, you are first. In your testimony, you reported that two-thirds of the Inspectors General list budgetary resources as their primary challenge in oversight. At the same time, you testify that in fiscal year 2012 there was a $17 return on every dollar that our government invested in IGs.

Well, first of all, this looks like a way to fix a national debt. How long does this go on before the return becomes less?

In other words, has anybody put any metrics to that to find out how much you are underfunded?

Ms. GUSTAFSON. Right. I do not think anybody has certainly put any metrics to effect.

I think, just speaking for my office, we have ways to go before we start seeing diminishing returns. For example, I think I am considered a mid-size office. Were I fully staffed and not subject to sequestration, I think I could have about 100 people.

In the meantime, the SBA loan portfolio is $100 billion, and small business contracting is, of course, 23 percent of all Federal contracts. And so, I think, just off the top of my head, 100 of us overseeing that is small.

Senator TESTER. OK. This is for anybody who wants to answer. It is kind of a lengthy question because it is multiple choice. OK?

When it comes to agency budgets for IGs, you must ask yourself, why are you being underfunded? Now is it because you do not have a seat at the table when agencies submit their budget? Is it a matter of not placing a high enough priority on IGs' duties when the

budget is being formed compared to other resources? Is there a conflict because some of the folks you are requesting oversight from will be part of the folks that you are tasked to do oversight on? Or, is it a matter of Congress not providing appropriate amounts of funding? You send the request in. We whack it and send it back at a lower level. As with all these, I mean, let us know where it is at. I mean, who wants to respond to that?

Ms. GUSTAFSON. Well, let me tackle it first——

Senator TESTER. Sure.

Ms. GUSTAFSON [continuing]. Especially as a member of the executive council and Chair of the Legislation Committee.

I have to say one of the things that Congress did for IGs that was a tremendous benefit—and I hate to say that because I worked on the IG Reform Act of 2008 because what that does for us, which is tremendously helpful, is Congress does get visibility into what the IGs are requesting for their budgets.

And so the way that the IG Reform Act is supposed to work is you will see what we believe—what we are asking for from the President and from Congress for our budget. It may not be the number that the President's budget—may be. It may be a different number. But you will get both numbers, which I think is tremendously helpful.

We also have the ability to note if we believe that the number actually requested for us is too low for us to perform the functions of our job. We are allowed to note that, write a letter, and that gets attached to the budget.

Quite frankly, the immediate issue that we have all been facing in the last few years has been the lack of an appropriation. I think what many of us have found is when you look—to get a little inside the Beltway, when you look at the marks that we are getting and when we look at the committees are offering us, those tend to be much better than what we are getting under a continuing resolution (CR), under a straight line and certainly under sequestration because, again, we are mostly salaries and expenses.

Just very briefly, the basic breakdown of my budget—and that is very similar to all IGs. Eighty-four percent of my budget goes to salaries and expenses. Ten percent is a fixed price contract for my financial statement audit of the agency. And 6 percent is everything else, which is every time my investigator needs to go somewhere to investigate a crime.

So, when you take 10 percent off the top, you are taking people. And we have been in that position for a while now.

Senator TESTER. OK. Does anybody else want to respond to that? Go ahead.

Mr. HOROWITZ. Just briefly, I have only been on 18 months, so I am only here on my second budget cycle. But, last year, what happened is we got the same 5 percent cut as everybody else did. So there was no distinguishing between IGs' budgets and other budgets.

As a result, that hits us for the reasons Peg mentioned. It is basically all salaries. It is hard to find other savings. We cannot just walk out of our rent space, our space, and all of a sudden save money.

The other is, also as Peg mentioned, even though our House mark and what we have requested is higher than 2013, and the House mark was higher, on a CR, I cannot hire at this point based on the hope that something will come through. I am either going to go maybe up on the House mark, maybe down if sequestration hits.

So, as a manager, I have to understand what my budget is, frankly, before I can start making hiring decisions.

Senator TESTER. OK.

Ms. NEUMAN. And, Mr. Chairman, may I answer that also?

Senator TESTER. Yes.

Ms. NEUMAN. The best way I can answer that is by just talking about our budget. If you take sequestration into account——

Senator TESTER. Yes.

Ms. NEUMAN [continuing]. The Privacy Office's Fiscal Year 2013 enacted funding level was $7.793 million, which is $614,000 below the level appropriated in fiscal year 2011.

And the main result of this has been our inability to backfill key positions that have been vacated due to attrition. And it has resulted in the loss of 4 privacy professionals, leaving 20 in my office and a backlog of—a FOIA backlog.

It is important to note we do not have a separate budget for oversight. Our Privacy Office gets one budget that goes to policy compliance and oversight. And with the funding levels being what they are, we are doing what we can with what we have, but it will—the effect is to have fewer people to conduct investigations, do privacy compliance reviews and investigations.

Senator TESTER. Maybe we should have an IG report on how much the fact that you guys do not have the personnel you need is costing the government—the IGs.

I mean I do not have a clue if anybody has ever done any work on that. You probably do not have time to, and nobody has requested it.

But the truth is if you are talking about $17 per dollar invested—and, Peg, you said we are nowhere near the point where we could top out—well, it is not good government. Let's just put it that way.

I will turn it over to Senator Portman. Senator Portman.

Senator PORTMAN. Thank you, Mr. Chairman, and thank you all for coming in.

I am probably going to start with Ms. Gustafson only in that you are chairing the IG Legislation Committee.

On the budget issue, I think Chairman Tester asked a good question, which is, are you at the table?

And I guess the other question is—and anybody should feel free to answer this. Assuming that you are at the table, I understand what you are saying about the Appropriations Committees being a better way to get your funding than through a CR because appropriators appreciate your work for the most part. I know sometimes they may disagree with you—and are likely to see the value of the return on investment you talked about.

But do you feel in a CR environment, and particularly a CR and sequester environment, that you guys are getting a disproportionate cut, and do you have any data to back that up?

Ms. GUSTAFSON. I think that the one thing that is troubling, too—and I cannot speak for every IG because every agency, I think, kind of treated it differently. But I think one of the things that was a source of some frustration for IGs, as Mr. Horowitz had mentioned, is, when these across-the-board cuts come, they are not supposed to be—and that is where we really do not have as much of a seat at the table because it is just a directive to do an across-the-board cut.

I think some of us found ourselves being subject to just the 5 percent cut whereas it seemed that the agencies were being told, do kind of a cost-benefit analysis; do not do just across-the-board, but figure out where this 5 percent should be applied.

I think sometimes that is not happening. I cannot say that this is not the same across every single agency, but I think that sometimes it is not happening.

I have found, for example—again, just anecdotally as far as the budget request—when the agency has been asked, find 10 percent but, again, do that kind of analysis, they take 10 percent from me.

Now I benefit again—and I think we all benefit—from the fact that I do not then submit a 10 percent cut to the President. I submit my number. And through the budget process, I, again, have been pleased—again, this is the appropriations process—with the President's request for myself.

I do not know if anybody else wants to add.

Senator PORTMAN. Yes, Mr. Horowitz.

Mr. HOROWITZ. I do feel like I have a seat at the table and am heard by the Attorney General, and I do not think that has been the issue.

I only have 18 months of experience, but the bigger challenge for me, frankly, has been living on a CR, not knowing if sequestration is going to go into effect or not, managing and figuring out whether I can or cannot hire because I am either looking at squeaking by next year or being able to hire and fill some of the vacancies, but I am going to be halfway through the fiscal year or close to that before I can do that.

And, frankly, with all the security clearances my folks have to go through——

Senator PORTMAN. Yes.

Mr. HOROWITZ [continuing]. It takes many months. There is such a lag time between losing someone and hiring someone. It is a tremendously difficult thing to manage.

Senator PORTMAN. So it is the uncertainty.

But you do not feel as though there is a disproportionate cut in your office as compared to other offices at Justice under sequestration?

Mr. HOROWITZ. No, I do not think I can fairly say that.

I think it is the bigger question of the across-the-board and the importance, frankly, as Peg said, of stepping back and saying, where is the value-add and where do we have the ability to cut, and making that analysis. That would, obviously, be helpful from my standpoint.

Senator PORTMAN. On the vacancy issue, quickly, we talked about that in my opening statement, and some of you addressed it briefly. But, frankly, I think that issue is a real concern.

The 2008 law, it seems to me, has been helpful. Do you agree with that?

Two thousand nine was kind of the low watermark, right? I mean, it was kind of the——

Ms. GUSTAFSON. Yes. I do not recall the historical level of vacancies. I do know the 2008 law addressed a little bit the idea of CIGIE keeping a list of potential candidates for IGs, which I know that this is done and that list is always available to both the President or to the agency, depending on how they are chosen and how they are hired.

But, I think it has gotten better in the recent past, but it does seem to fluctuate.

Senator PORTMAN. Do you support what we are doing here in terms of confirmations on IGs? Do you have thoughts on that?

Ms. GUSTAFSON. Well, I think it was very heartening, if I can speak for the IG community, that two of our very well respected IGs were just confirmed very quickly for State and for Defense, and I think that has to have been seen as a favorable process.

Again, it seemed to me that the nomination process went very smoothly. From the day of intent to nominate and to the day they were confirmed was a fairly short amount of time——

Senator PORTMAN. Yes.

Ms. GUSTAFSON [continuing]. Which is, obviously, a positive thing.

Senator PORTMAN. And this Subcommittee and this Committee are sort of the champions of trying to get our IGs through. So, when you have issues, I hope you, as the Chair of the Legislation Committee, will come to us.

I think one thing, if you can get it in the record, that probably would be helpful, is to say what is the impact of not having a permanent IG?

In other words, if you have Acting IGs, how does that affect the morale of the office? Is there a wait-and-see-what-happens attitude among folks when you guys are dealing with your counterparts in the agency?

In other words, this person is not going to be here forever. Why don't I just see if we can wait him or her out?

Ms. GUSTAFSON. I think it is hard to make a universal claim about what the effect of an Acting IG is because, quite frankly, it seems to me, having been even on both sides, having worked on the IG Reform Act and now having been an IG for over 4 years, an Acting IG has all the ability to be as independent as a permanent IG, which is to say the great things that the IG Act does that gives the IG that independence are available to an Acting IG as well as a permanent IG. So, there is not a structural problem with that.

As to the other part of your question, whether some things are waiting for the permanent person to come, I think that would also depend on the Acting IG. I know that when I came in to my office that my Deputy Inspector General (DIG) had been Acting for a while. I think, in general, the place was running quite smoothly.

Quite frankly, there were some policy decisions that I made when I came in, to take it in a different area. There were some changes I made.

But whether things were being held off, I think, depends on—it really gets down to the individual office and how that Acting IG is doing.

Senator PORTMAN. OK. I would think continuity would be affected, and just accountability.

Ms. Lerner, you mentioned you are protector of the merit system laws.

And, as you know, Senator Tester and I have recently been working with you.

And you sent a letter to the DHS Acting Secretary, Beers. So the Department of Homeland Security does not have a Secretary or a lot of positions filled, but the Acting Secretary was asked to provide you information regarding this recent report you guys did administratively uncontrollable overtime (AUO).

And, as you know, this administratively uncontrollable overtime is supposed to be very limited. In fact, the statute says it should be used for irregular and occasional circumstances only, such as if a failure to stay on duty would constitute negligence, so a very narrow kind of overtime.

And, looking at it, you determined that these improper claims of overtime have reportedly cost the Federal Government up to $9 million annually at 6 DHS offices, reported by whistleblowers to you. The amount of annual abuse of this is unknown because we do not have the information yet.

Senator Tester is holding a hearing on this in the next month, and we look forward to that hearing, but just a couple process questions for you on how organizations respond to situations like this because we are concerned about the lack of response.

The statute that governs these responses requires agencies to describe any action taken or planned as a result of the Office of Special Counsel investigation. To me, the response to you from DHS seemed totally lacking in detail, specifically, anything about any disciplinary action against employees. And I guess we can either assume that there were not any actions taken or that they are not telling you what actions were taken.

Can you comment on this briefly?

I want to get to my colleagues' questions. So we can maybe do a second round on this. But, just briefly, does this happen often, that agencies do not fully respond to your requests, and do you think it is consistent with the requirements outlined in the statute—the way they responded from DHS?

Ms. LERNER. Well, I think there are several parts to your question. Let me sort of address the process one first.

You are absolutely correct that the agency has to respond to us when we send over a disclosure, and the type of response that we got from DHS was actually pretty much on par, if not better, than some of the responses that we get because DHS did confirm the allegations that the whistleblowers made. They did not deny the allegations at all.

So I took some measure of comfort from the fact that they admitted that they had a problem and, at least on paper, said that they are taking responsibility for fixing it.

Now the problem is they said the same thing 5 years ago. A very significant portion, like maybe a quarter, of the report that we got

back recently was basically cut and pasted from the report that we got back 5 years ago when the same allegations were sent over there for investigation. So not much has changed.

The other thing that has not changed, as you mentioned, is the detail about what they are going to do to fix the problem. The action plan, if you will, that they gave us this time mirrors the same steps that they said they were going to take 5 years ago, with the exception of a new video that they plan to show to all employees.

So it is a little bit bare-bones in terms of what they are going to do to fix this problem.

They have said that they are going to do a full audit of this problem. So let's hope that that helps expose both how deep the problem is—how widespread it is—and how they might fix it.

Senator PORTMAN. Let me cut you off there because I want to get to Senator Johnson's questions, but if we can do a second round, I will have some other questions for you about how they responded.

Ms. LERNER. Sure.

Senator PORTMAN. Thank you, Mr. Chairman.

Senator TESTER. We will be doing a second round. Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman.

Ms. Gustafson and Mr. Horowitz, I guess I would first like to start out asking, how do you prioritize your cases for investigation?

Ms. Gustafson, we will go with you first.

Ms. GUSTAFSON. I have about 45 criminal investigators. And they are spread out throughout the country. So I think there are any number of factors go into how they are prioritized, including the caseload of the investigators that I have.

My criminal investigators work very closely with DOJ, U.S. attorneys, assistant U.S. attorneys, and very often the decisions on whether a case is a go or no-go often is dependent or contingent upon talking to DOJ, seeing the likelihood of that case, of course, being accepted for prosecution because it is important that we do that.

So, in addition, of course, certainly the amount of loss is always a factor in any case. For my investigators, again, the two biggest things that we are looking at are loan fraud in the SBA lending programs and then small business contracting fraud.

And so, one of the emphases I made was to reemphasize a little bit the contracting fraud. Those cases sometimes went a little bit by the wayside, and so we put more of an emphasis on that.

And I think that that plays a part in that, which has resulted in some of our biggest cases, including a $100 million contract fraud case, with a billion-dollar contract that was about to be awarded fraudulently that we had a couple years ago.

So there are any number of factors.

Senator JOHNSON. So, I mean, likelihood of prosecution or quality of the prosecution, then the dollar amount.

Mr. Horowitz.

Mr. HOROWITZ. If it is a criminal allegation involving Justice Department employees or Justice Department funds, we will investigate it. We will open an investigation and go forward.

I have had occasion where I have had to call the U.S. Attorney because my personal view, having been a prosecutor on corruption

cases before, is the dollar value in a corruption case should not matter, like it should in many others. If a public official is taking money, that warrants—and you can prove it as a crime—that warrants prosecution.

In the noncriminal context, because we get thousands of various pieces of information coming across, first off, as I mentioned earlier, we do not have authority over attorney misconduct in the course of attorney work. That is a problem from our standpoint. So those cases go back to the Department. They investigate themselves in that instance.

For non-attorneys, we will look at the seriousness of the allegation. We take high-level official misconduct. So GS–15 and above—generally, we will look at that.

And then, separately, we assess in the remaining cases, what is the need for independent oversight? What value do we bring as an independent oversight authority to look at that?

Senator JOHNSON. OK. I just kind of want to explore your relationship with the agency and the Department and your independence.

Let me first ask, what is—and I realize this is kind of hard to summarize or typify. But, what would be a ballpark in terms of how long you want to take on an investigation?

I mean, how quickly do you want to get through something? What would be an average length of time for an investigation?

Mr. HOROWITZ. Well, let me speak from our standpoint. We have such a wide range, frankly, of allegations. We have some in the prison, and we have the prison system. We might have a video that will take a very short time. Other more sophisticated, grant-related frauds that could require us to go administrative or grand jury could take months and years. And we do not control some of those because those then to go the prosecutor, and they have to bring them.

Senator JOHNSON. OK. Well, let's talk about timing of the release of a report. Who is in charge of that? Is that strictly a call made by the Inspector General's Office?

Mr. HOROWITZ. In a noncriminal case, we would make the call. In a criminal case, obviously, it is going to be the indictment, and that is the prosecutor's control.

Senator JOHNSON. In terms of the reports you issue—and I will ask both of the Inspectors General this—what is the appropriate relationship between yourself and the agency or the department you are investigating?

Mr. HOROWITZ. From our standpoint, when we do an investigation, we do it—of the Department—if it is a third-party, for example, we might have the FBI where we——

Senator JOHNSON. I am just talking about if you are talking about your Department.

Mr. HOROWITZ. Right. Internally, we do it ourselves. We talk about it ourselves. And, when the time comes, like in Fast and Furious, to issue the report, we send the proposed final report for comment, and that is when the Department gets its first chance to comment.

Senator JOHNSON. So it would be totally inappropriate for the Department to comment or see the report ahead of time, before it is released?

Mr. HOROWITZ. We will give them a chance to review our—for example, in audits, investigations—audits and reviews—let me do audits and reviews.

We will give them a chance to review and provide us, in some instances, with informal comment but always with formal comment, which is what you see attached.

Senator JOHNSON. OK, but that would be a comment. It would be an addendum to the report.

Would they be changing wording in your report?

Mr. HOROWITZ. They would not have authority to change wording.

In audits, for example, we will often sit down with the component and say, here is what we found. Here is a problem.

For example, ATF undercover operations that we just did, we found unreconciled $100 million worth of cigarettes. We went to the Department when we heard about that to alert ATF and the Department that they needed to fix the problem.

Senator JOHNSON. OK.

Mr. HOROWITZ. So, for example, in that instance, they would know even earlier in the process.

Senator JOHNSON. But the department or agency would not change the wording of your report.

Mr. HOROWITZ. We would not let them change the wording.

Senator JOHNSON. They could read——

Mr. HOROWITZ. They could comment to us.

Senator JOHNSON. So it would be totally inappropriate if an agency or a department changed wording with a report?

Mr. HOROWITZ. I would not allow the Department to edit my document.

They might give me comments. They might say I have it wrong. We would then sit down and talk about it internally, and we make the decision.

Senator JOHNSON. Ms. Gustafson, do you agree with that?

Ms. GUSTAFSON. I do agree with that, again, and I have to say for myself I am basically talking about the audit context.

My criminal investigators, again, that we are talking about——

Senator JOHNSON. OK. I am talking about a report on your agency or your department.

Ms. GUSTAFSON. Right. The reports that we issue are done by us. Certainly, there is always a lot of communication between the agency.

There is no question, though I am not an auditor, that they are probably suggesting language. But, do they get to dictate language and edit and then have final say? No, absolutely not.

Senator JOHNSON. Would either of you ever—or would it be appropriate for you—to utilize the agency or the department's counsel in any capacity?

Mr. HOROWITZ. The Department actually does not have a general counsel. It has the Office of Legal Counsel, and we would not necessarily go to them for guidance or legal advice.

Senator JOHNSON. Ms. Gustafson,

Ms. GUSTAFSON. No. As the IG Reform Act notes, we have our own counsel.

Certainly, OGC always has their own opinion of the legal issues in our audit reports, and we get to hear those, but we do not rely on them.

Mr. HOROWITZ. Let me echo that. I go to my general counsel regularly on issues. That is where I would go.

Senator JOHNSON. But, again, your general counsel in the IG's Office, not the Department's.

Mr. HOROWITZ. The IG, correct.

Ms. GUSTAFSON. Yes.

Senator JOHNSON. OK. Thank you.

Senator TESTER. OK, I want to talk a little bit about overclassification. It is something both, quite frankly, of information and of positions. It has something that has come to light in a number of different areas. It is something that I actually feel very strongly about because it compromises transparency and it impairs our ability to perform quality oversight.

The question is, have you run into situations where you are not able to get information due to overclassification?

Anybody who wants to answer that can.

Ms. GUSTAFSON. First off, I am supposed to, under the IG Act, have access to anything that I need from my agency, and so what they are classified as should not dictate what I get to see or not see. Section 6 of the IG Act is very clear about that.

Senator TESTER. So, if it is classified as being secret information of any type, you still have access to it?

Ms. GUSTAFSON. I have. There are people in my office who have. For example, I have a top secret clearance. There are people in my office—I mean, we have people who have certain clearance levels just as the agencies do.

Senator TESTER. Sure.

Ms. GUSTAFSON. And, for example, if we have worked on audits—we have done audits on DOD projects, for example.

Senator TESTER. Sure.

Ms. GUSTAFSON. I had a team of auditors who actually I stole from DOD IG, who came with top secret clearances. If we needed to see that information, they would have the auditors who would see it because they would have the appropriate clearance levels.

So we have not encountered that problem.

Mr. HOROWITZ. In terms of the Department saying we cannot look at classified information, we have not had that problem.

We have had discussions, though, as I referenced in my testimony, to a question being raised whether we are, for example, allowed to see raw FISA data, which—as you know, we do many reviews related to FISA. That would be problematic for us.

We have not had it withheld from us. We have worked through the issues. But that is, for example, one of the issues that we occasionally deal with.

The other context that this comes up is when we want to issue a report we fight very strongly to have the report go public in as great a detail as it can, and we often get faced with, in our view, the initial response being overclassified, whether law enforcement-sensitive, which is a separate category, or actual classification. We

end up pushing back very strongly and having in many instances, I will call it, a robust discussion internally.

We ultimately do not control the final decision because it is not our information, but we do push forward very aggressively in ensuring that when we think there is an overclassification in response to our report we fight internally and often elevate it within the Department and frequently prevail, frankly.

Senator TESTER. Anybody else want to respond to that? [Pause.]

So let me ask it this way. From your answers—do not let me words in your mouths—I am not hearing that there is any impediment as far as getting information regardless of the classification.

Ms. GUSTAFSON. I am not aware of impediments regarding classifications.

Senator TESTER. OK.

Ms. GUSTAFSON. I am aware there are sometimes IGs—and I think Mr. Horowitz has some of his own specific examples—how some laws are thrown up, saying—thrown up to them, saying you do not have access because of this specific law, and then IGs need to work through that.

Again, the IG Reform Act is supposed to give us access to that, but I have not heard of classification being an issue.

Mr. HOROWITZ. Right. As Peg said, it is an issue that has been thrown up. We have had to work through several and various areas, not necessarily the classification issue, but on the raw FISA information area—it has come up. It takes many months.

To the point of how long does it take sometimes to do our views, they are greatly impacted by those back-and-forths. So it can take months.

Senator TESTER. OK. Ms. Neuman, your office handles privacy policy within DHS. It has sought to create an environment in DHS where neither privacy nor security is compromised—an admiralable task, tall task, especially in an agency like DHS that has something like 22 agencies in it. Many interact daily with literally millions of Americans.

How successful have you been?

Ms. NEUMAN. Well, in the short time I have been here, I have to say that I think we have done a really good job. We have been very successful. We work very closely with our component privacy officers and privacy points of contact during the development of programs and systems to build privacy in on the front end, to build privacy protections in on the front end.

All of this is documented in our compliance documents, the PIAs I mentioned earlier, which serve a really important—two very important functions. One is transparency to the public so they know what information is being collected and how it is used, but it is also used—these PIAs are also used to help provide benchmarks for the oversight process so that the privacy risks are identified.

Through the PIA process, we work to develop very strong mitigation mechanisms to protect privacy, and then we refer to those benchmarks during PCR reviews and other assessments of how effective the privacy protections have been. And we update the PIAs as necessary. They are posted on our Web site.

So you are right; it is a very challenging job, but our mission is to sustain privacy in the systems and programs that the Department is implementing and developing.

Senator TESTER. Can you give us an example of where your office has interjected itself into the process to voice its concerns over privacy?

Ms. NEUMAN. Well, there are a number of programs that are developed to collect information, whether it is at the border or from passengers traveling into the country, students coming in on visa programs. And we are very careful that the information is collected only for a specific purpose. We pay very close attention to retention periods so that information is not collected longer than is necessary to accomplish a purpose and that access to that information is really limited to people who have a need to know that information or/and a need to use that information to carry out their responsibilities.

Senator TESTER. OK. Michael, the same series of questions as far as privacy goes—is there a time where you have been able to be successful in balancing that, or is that not an issue in your Department?

Mr. HOROWITZ. The privacy issue for us really does not arise in my office.

Our view is we are independent. We make our own decisions on those issues.

We push very strongly to put forward publicly, as long as it is legally allowed, and obviously, the Privacy Act plays into this. We want to be transparent. We want our reports public. We want the information posted on our Web sites.

The issue comes back in pushing on what is law enforcement-sensitive and some of the other issues that we struggle with.

Senator TESTER. All right, Senator Portman.

Senator PORTMAN. Ms. Lerner, going back to the previous questions we had about administratively uncontrollable overtime, your response sort of surprised me because you said you thought this was about par for the course in terms of the response from DHS. You were pleased that they did not deny the allegations; in fact, they admitted them. You also noted that they had essentially done that 5 years ago and that you were still concerned about the kind of follow-through you would get.

Let me just ask you specifically about whether you think the current statute gives you the authority you need to get the information that you need.

The statute is 5 U.S.C. Section 1213(d)(5). It says, agencies are required to describe any action taken or planned as a result of the OSC investigation.

However, it uses the term, such as, and it says, such as changes in agency rules.

The restoration of any aggrieved employee is what we were talking about earlier, that you do not know whether there has been any disciplinary action taken.

Ms. LERNER. Right.

Senator PORTMAN. Disciplinary action taken against any employee, referral to the IG of any evidence of criminal violation, changes in rules, and so on.

Do you think it would be helpful for you, in terms of getting the responses you feel that you need, to have that a requirement in the reporting in the statute, or do you think you have the authority that you need to be able to get to the bottom of these?

Ms. LERNER. Well, unlike prohibited personnel practices, where we have, for example, a retaliation case after someone comes to us with a disclosure—and we do have some of those in the DHS matter too—the agency does have to let us know what actions they have taken or will take as part of an agreement with our agency. And I think that is very helpful.

Of course, in that context, we have the ability to actually prosecute cases to the MSPB and either require the agency to take disciplinary action or make sure that the whistleblower is made whole if they have been retaliated against. So we can require the agency to take remedial action.

We do not have that same ability in the disclosure context under, as you said, 1213(d). We do not have independent investigative authority.

In assessing whether the report from the agency is reasonable or not, one of the things that we look at is what remedial action they have taken.

So the reason that I found the report inadequate was not because they did not come up with the right outcome in terms of verifying the allegations; they did.

The reason I found it inadequate was because they had not taken effective remedial action and because their steps for solving the problem were not appropriately outlined, and it left me with the concern that they did not have the ability or the willingness to take corrective action.

Senator PORTMAN. OK, given the history, but I guess what I am questioning is whether you even have adequate information to know whether they have taken remedial action because they were not required to tell you.

Ms. LERNER. Well, they were not required to tell me if they took disciplinary action. They were not required to tell me if they were trying to figure out whether the overtime that was being taken was actually fraudulent overtime versus just inappropriate overtime.

They are required to tell me what steps they are going to take to solve the problem.

Senator PORTMAN. Like the video.

Ms. LERNER. Like the video.

Senator PORTMAN. Yes.

Ms. LERNER. They outlined a few steps.

Senator PORTMAN. But not disciplinary steps and so on.

Ms. LERNER. That is right.

Senator PORTMAN. We will get into this more in the hearing, and I just wanted to prepare us maybe better for the hearing by getting your input on that.

Ms. LERNER. Sure.

Senator PORTMAN. Our job is, among other things, is to look at legislation. So we are going to be looking at that code section. If you have additional thoughts, I hope you will let us know.

Ms. LERNER. OK.

Senator PORTMAN. On whistleblowers, we talked a little bit about this. Mr. Horowitz, maybe you are the right person to talk to since you have had some experience here.

In 2006, the IG at Justice testified before another congressional committee. This is Glenn Fine, and he said that—this is in the context of FBI reprisals against whistleblowers by revoking an employee's security clearance. You are probably familiar with this.

Mr. HOROWITZ. Mm-hmm.

Senator PORTMAN. He testified, "The IG would have authority to investigate an allegation that an employee's security clearance has been revoked in reprisal for protected disclosure under its general authority to investigate allegations of misconduct, fraud, waste and abuse in the Department."

He also stated that the FBI official said that they were not familiar with any case in which an employee alleged that revocation or denial of a security clearance was in retaliation for protected disclosure.

A couple questions—one, do you agree with IG Fine's point on the authority of your office to be able to do that, and are you aware of any instances in which an employee has alleged that revocation or denial of a security clearance was in retaliation for a protected disclosure?

Mr. HOROWITZ. I do agree that we would have the ability to go forward as he suggested.

I do not, as I sit here, recall any such instance in my 18 months on the job, but I can certainly go back and check on that.

Senator PORTMAN. Have you ever investigated an allegation of reprisal based on a security clearance being suspended or revoked?

Mr. HOROWITZ. We do have several reprisal cases going on, and I would have to, frankly, go back and see if that was one of the components of the claim. There may be one, but I would want to double-check.

Senator PORTMAN. OK. I think it would be helpful to me if you would get back to me on that.

Mr. HOROWITZ. I will do that.

Senator PORTMAN. Given some information that we had received, we just want to try to confirm or determine whether it is an issue or not.

On the privacy issue, Ms. Neuman, you responded to the Chairman's questions about how your office operates within DHS. You were pretty positive about that and the experience you have had there.

Can you give us a specific example of where your office has interjected itself into the process to voice a concern over privacy?

Ms. NEUMAN. Let me answer the question this way. I am not sure that I would see us as interjecting ourselves. We foster a culture of privacy throughout the Department. And included in the context of oversight, part of that culture is encouraging—in fact, requiring—the reporting of privacy incidents.

We do so in a way that encourages people to come forward without fear of reprisal or humiliation, and we would initiate an investigation if we found evidence or allegations of really egregious conduct or willful noncompliance with Department policy or directives.

We work with the components to address problems. We often find that we do not have to get involved or initiate resource-intensive full-scale investigations. We are really able to address issues throughout privacy compliance review process, which is a collaborative process that enables us to make—to validate that the privacy requirements are being adhered to.

So I see us as really working collaboratively throughout the Department and not interjecting ourselves absent the need to do so for really egregious conduct. And we have initiated three investigations where we felt it was necessary to investigate conduct that was brought to our attention or that we otherwise discovered.

Senator PORTMAN. OK. If you are at liberty to provide us that information, that would be helpful.

Ms. NEUMAN. One of them was public.

Senator PORTMAN. No need to do it now. We want to get on to Senator Johnson's questions.

Ms. NEUMAN. Certainly.

Senator PORTMAN. But if you would not mind in writing to provide that to the Subcommittee.

Ms. NEUMAN. Certainly.

Senator PORTMAN. Thank you very much.

Senator TESTER. Thank you, Senator Portman. Senator Johnson.

Senator JOHNSON. Thank you, Mr. Chairman.

Ms. Gustafson, in your position as Chair of the Legislation Committee of CIGIE, I just kind of want to walk through a couple questions.

First of all, when there are allegations of wrongdoing or reports of wrongdoing in the Inspector General's Office, can you just quickly walk us through exactly how CIGIE handles those?

Ms. GUSTAFSON. So the IG Reform Act of 2008 codified the Integrity Committee, which I will tell you existed before the IG Reform Act. The Integrity Committee was in existence.

And it is there specifically to investigate allegations of wrongdoing by IGs or by those direct reports of IGs where an investigation could not be done by the IG Office due to a conflict, our head of investigations or our DIG, so that when an allegation is received—the Integrity Committee has a Web site and a number.

Some people would report those allegations directly to the Integrity Committee, which is chaired by the FBI. And then the Integrity Committee is comprised of the FBI, four Inspectors General chosen by the Chair of the Council and also Office of Special Counsel and Office of Government Ethics.

The FBI chairs that and takes those allegations, and it goes through a process of determining whether it should be sent to Justice, determining whether an IG needs to answer it.

If the allegations come through some other way—sometimes I believe these allegations are sent to CIGIE themselves. CIGIE has an office, seven employees, an executive director.

I think sometimes the allegations are conveyed to the Chair of the Council. Those are always sent right to the Integrity Committee for the process. All allegations are processed the same way and go through that process.

I do not know if you want me to walk through that process a little bit.

Senator JOHNSON. No, let's try talking about it specifically. Has CIGIE received allegations from the then-Acting and now-Deputy Inspector General in the Department of Homeland Security?

Ms. GUSTAFSON. Well, unfortunately, I do not know the answer to that question because I certainly have not. I am not being facetious. I do not know.

I know this is has been a topic of discussion.

I believe that to the extent that any allegations have been made and they have been sent to the Integrity Committee, I was not——

Senator JOHNSON. You would have no knowledge of that then?

Ms. GUSTAFSON. I have no personal knowledge of that.

My understanding is any allegations received by any—about any IG are sent by CIGIE which, again, would be the Executive Director or the Chair, to the Integrity Committee.

But I do not have personal knowledge of that. I was in a briefing it was—where they talked about that is the process they would have taken, but I do not have personal knowledge of what IG——

Senator JOHNSON. Well, let me ask anybody in the panel. Is anybody on the panel aware of any allegations of wrongdoing on the part of now-Deputy Inspector General of the Department of Homeland Security? Anybody aware of that? Ms. Lerner.

Ms. LERNER. Senator Johnson, I do sit on the Integrity Committee. I am recused from any matters involving the DHS IG because the same allegations are at my agency. So I cannot speak to you specifically about anything, and I probably could not in this public forum anyway.

But I can confirm that allegations were at least being considered. I do not know the status now. As I said, I am recused.

Senator JOHNSON. Anybody that is not recused that can answer the question? [Pause.]

Then I have no further questions.

Thank you.

Senator TESTER. Wendy, you cannot get off. The technology and how IGs throughout government are utilizing it—how would you grade them on utilizing technology in their jobs as Inspectors General, whether it is getting to the problem of problems or getting information out to the citizens?

Ms. GINSBERG. If you are asking about the Inspectors General specifically, the best resource for that that I could find was the Council of the Inspectors General on Integrity and Efficiency had their own report on the use of new media. And, as I said in my testimony, they did not have a high level of respondents for that particular ask of information on how many IGs were using new media, but only 26 of the 72 existing IGs responded that they were using any form of new media whatsoever.

Senator TESTER. So what you are really saying is that they would have been utilizing it they would have probably responded.

Ms. GINSBERG. My thinking on it was if they were doing something incredibly innovative they probably would have responded.

Senator TESTER. OK. Let me ask you about information being put out there for public consumption when there is so much of it that actually dilutes its effectiveness.

Is there anything that we can do—quite frankly, because transparency is a big thing in any part of government—that could help

make it so it is more accessible to folks? It might be out there, but it still might not be accessible.

Ms. GINSBERG. Well, I think the Smart Disclosure Initiative is one way. The Administration is trying to tackle exactly that problem, that you just cannot pour reams of data out there and expect that every user who has an interest in finding a particular data point can find that data point. You get lost in the big haystack and cannot find the needle.

But Smart Disclosure is an attempt to put this data in machine-readable formats that allow interplay between sets of databases. It is a way to try to get through and find at least a few needles that might fit together and create something that is more usable to individuals and the public, so they can assist in Federal oversight, or create really new, incredible apps that help people in their daily lives.

Senator TESTER. These guys have enough to do, plus, with short budgets and sequestration.

Who would be responsible to give some guidance on that so that—whether it is apps or whether it is——

Ms. GINSBERG. It has historically been communicated through—the Office of Management and Budget has come out—they have been in charge of creating a lot of the public-facing Web sites with the Electronic Government Fund that is administered through the General Services Administration (GSA).

Senator TESTER. Yes.

Ms. GINSBERG. So I think that they have done a lot of writing of guidelines and memoranda to help agencies figure out how to frame what data sets they should be releasing in making information more accessible to the public.

Senator TESTER. OK. This next couple of questions are for the Inspectors General. We rely upon your oversight work to shed light on misconduct and waste in the agencies. Who is ultimately responsible for policing the work that you do?

Ms. GUSTAFSON. Well, it depends on what you mean by policing, but as I—because there are a couple different——

Senator TESTER. Well, let me put it this way. If you have an IG that is really not doing their job——

Ms. GUSTAFSON. Right.

Senator TESTER [continuing]. Who checks? Where is that box checked at?

Ms. GUSTAFSON. Well, just to reiterate, first off, as far as allegations of wrongdoing or things that are serious enough to suggest that an IG should not be an IG, that is the Integrity Committee. Those referrals are made to the Integrity Committee.

And, just so you know, in the context of that process, DOJ Public Integrity Group also is referred to anything where there may be allegations of criminal wrongdoing.

Senator TESTER. Yes.

Ms. GUSTAFSON. As far as making sure that our work is up to standards, all of our offices are subject to peer review. Our audit shops receive a peer review every 3 years from another audit shop. Those of us with law enforcement authority undergo a peer review as well from another IG every 3 years.

But, as far as whether we are being as effective as you want us to be, we are reportable to Congress, and of course, I am reportable to the President.

And whether I am doing the best job, in general, what that is, is that is up to you to make hay about it if you do not think so and the President to remove me if he does not think so, with 30 days notice, too, as to why.

Senator TESTER. Yes, but here is the problem from our perspective, and I do not want to give you guys a way out here, but unless somebody is doing the evaluation of you, I guarantee you—well, maybe Senator Portman can, but I cannot evaluate the work that you are doing. I do not have the skill set to do that——

Ms. GUSTAFSON. Right.

Senator TESTER [continuing]. In a way that is fair and effective.

Ms. GUSTAFSON. Right.

Senator TESTER. So where do we go to get the information?

Ms. GUSTAFSON. Well, again, I think that if it is a function of whether we are working under standards our peer reviews are posted on the Web sites, and whether we pass peer review.

But, as far as whether we are up to snuff, I go to hearings. The Small Business Committee will have hearings very regularly where they will, I think, have a little bit more insight into whether I am doing the job that they think I should be doing just because of, obviously the subject matter.

I am sure Mr. Horowitz has the same type of thing.

But, as far as the effectiveness, we issue semiannual reports that talk about the accomplishments that we have made.

One of the things that I think is often very useful myself is we issue the top management challenges from the agency. That is a report that we issue annually. Personally, I think that that is a good arbiter of how effective we are because the agency has to—I think it shows whether the agency is listening to us, paying attention and whether the big problems are being fixed. I think that is often sometimes a good measure.

I think there are any number of things that way.

I do not know, Mr. Horowitz, if you have something to add.

Mr. HOROWITZ. And, just briefly from my standpoint, frankly, having been on the job for 18 months and seeing what we can do and the impact we can have, if you are not seeing strong, solid reports from IGs, they are probably not doing all they can because there is a fair amount of follow-up work, audits, investigations and reviews that can be done that, if they are done aggressively, will find things.

And so I think one of the things that is very important is getting those reports out publicly and getting them out to Congress.

And I think also, frankly, from the discussion we have had today, we in the CIGIE community need to be as transparent as we are with our own agencies. We, as a community, should be putting out there what we are doing to self-police and self-patrol so that taxpayers know what we are doing and whether they are getting value for what we are doing.

Senator TESTER. OK, Senator Portman.

Senator PORTMAN. Thank you, Mr. Chairman.

And thank you all for being here today. We will continue to be in touch with you and your colleagues.

To Ms. Ginsberg, I have to ask you some questions here because you kind of left out earlier. The Chairman started with his, so I will, too.

On this whole issue of technology, we are in the middle, as you may know, of looking at security clearances—this Subcommittee. This comes out of a longer interest but particularly the horrific events at the Navy Yard and how that guy got his clearances. We had been into it a little bit on the privacy side, protecting some of our most important government secrets.

And what we are trying to do is figure out how we can, on the security clearance front, get better access to databases, sometimes within the government, sometimes outside the government, for more expedited clearances, more thorough clearances and that sort of thing.

So just hearing your testimony and your response to the Chairman's other question, can you tell us more about how the Inspectors General should appropriately access data?

You talk about the fact that there are so much more data out there and that that is good because the public now knows more about how their government operates.

When I was at the Office of Management and Budget, we put all grants and contracts online, and I was a strong proponent of that. That actually came out of legislation in this Committee as I recall.

But the reality is someone has to analyze it and do the sort of next-level analysis to determine whether this information is the right information coming from agencies—in other words, if it is accurate, if the agency is doing what it says it is going to do.

And also, I think there is a responsibility among the IG community to look beyond the data and sort of say, is this the right data?

In other words, you might have a whole lot of data on certain issues out there from, say, the Department of Justice, but other stuff—I mentioned whistleblowers earlier and some of the reprisal issues—that might not be out there. So how to sort of balance that out?

Anyway, what are your thoughts on that, Ms. Ginsberg, and can the IGs use data more effectively to do their important jobs?

Ms. GINSBERG. I think it is certain that data can be helpful to figuring out the best policy options and the oversight process generally. But I will say that more data does not necessarily equal better; more use of new technologies and new media does not necessarily mean you are going to better execute your mission.

You have finite resources. You have to spend them in a way that is the best way to execute your mission. So just going out here to find as many databases that you can get access to is maybe going to encumber your mission more than anything else. You are just going to get more background noise than the information that you actually need to execute what you want to execute.

So I think it is more of a strategic game about figuring out what media might best suit your needs.

And I think earlier Ms. Gustafson talked about the issues that exist with the Privacy Act that inhibit data matching in some cases for IGs. They cannot get access to one data set that might provide

them and tell them whether applicants for another entitlement, whether they are providing accurate information to get that entitlement. And you can cross data sets there. That might be a really great use of a new database that an IG can acquire.

But to just start using Twitter, to start using Twitter might not be the best use of resources of an IG.

Senator PORTMAN. Yes. And I think it is an opportunity but also a challenge, including, as the Chairman said, just the inability to have adequate staffing to do your current job, much less to be able to look through these troves of data.

And there is a lot out there, but how much of it is really useful is the question.

And then some of it is classified or at least not public, and so that is a challenge for you guys to get a hold of that.

Any other comments on that?

Mr. Horowitz, you seem like you have a comment.

Mr. HOROWITZ. Let me just add. We did a report shortly after I got there on referencing checking, vetting of applicants at the Department, and the Department was not doing a very good job of that. Put aside, separately, just the security clearance and background check. Good old-fashioned reference checking is something the Department was not doing.

And I am happy to send a copy of the report up to the Committee because that is something that should be done. There is really not much that it takes to get references and followup.

And on the data issue, it is a big issue for us. We look, for example, at travel card purchases. We have our fraud detection office and my office looking for anomalies in that data, seeing if they can get out of there what would otherwise be subsumed. It may be a very small charge, but if you can find a couple of small charges——

Senator PORTMAN. It might show a pattern.

Mr. HOROWITZ [continuing]. That are fraudulent, it might show the pattern.

And so we try and do that, but it is very hard.

Senator PORTMAN. Well, thank you all very much for being here.

Senator TESTER. With every answer comes another question.

I mean, the truth is you are exactly right; they do need to do the followup on the background checks. If they do not, we end up in a very difficult situation.

I would hope that you have the ability—the IGs—to get people's attention if they are not doing their job so that, ultimately—well, I have a different perspective. I do not think there is any tolerance for folks who do not do their job in this particular area. They should be gone.

And I do not know if you have that ability to make those recommendations or not.

Mr. HOROWITZ. We absolutely make the recommendations, and one of the things that we try and do is followup on our recommendations. We have hundreds of open recommendations in the Department in a variety of areas——

Senator TESTER. Right.

Mr. HOROWITZ [continuing]. Not just in this one.

But one of the things that is incumbent upon us is to do a better job regularly following up on those recommendations and reporting

to the leadership of the agency and to Congress on what the status of those open recommendations is because changes—finding the problem is not—is 10 percent of the issue. Remediating it is the key part, frankly.

Senator TESTER. Yes. And along those lines, if we want to make your job less necessary in the future, we need to do prevention up front. From my perspective, one of the best ways to stop waste, fraud and abuse is drop the hammer on the folks who are doing it.

Any other ideas in prevention that would work?

Ms. GUSTAFSON. I think that there is definitely dropping the hammer certainly in a lot of these contexts. For example, again, we do a lot of Federal contracting work, and that is a fairly small community. When we are able to get good successes in contractors being debarred, contractors being prosecuted, people know that, and that message gets out.

I also think that you are right; there is also a need to be proactive and work with the agency, make sure that it is best to get the money before it goes out the door——

Senator TESTER. Right.

Ms. GUSTAFSON [continuing]. Rather than to try to get it back. And I do think that that is something that all IGs are working on and working closely with agencies, to kind of—to prevent the fraud and the waste before it occurs.

Senator TESTER. OK, I have a few other questions that we are probably going to enter for you guys to respond to at a later date because this hearing has gone quite a while.

I want to thank you all once again for being here.

Senator Portman, do you have any closing remarks? [Pause.]

We have covered a fair amount of ground here today, and I think it is important that we cast a light on the challenges of our oversight workforce and the opportunities we have to increase efficiency and effectiveness of government. It is all something we all want to see happen.

As I said at the outset, public trust in the Federal Government is waning, and we certainly have a lot of work to do to restore that faith. And we can start by moving forward on some of the ideas that were put out for us today and support the efforts to shed light on government and help ensure taxpayer dollars are being spent responsibly and productively.

I certainly look forward to working with the folks not only on this Committee and Ranking Member Portman but all of you and the other folks that work in the different IG offices. I think it is the only way we will tackle the problems.

The hearing record will remain open for 15 days for any additional comments or questions.

Once again, I want to thank the panelists.

We are adjourned.

[Whereupon, at 4:09 p.m., the Subcommittee was adjourned.]

APPENDIX

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

STATEMENT FOR THE RECORD OF

PEGGY E. GUSTAFSON
INPSECTOR GENERAL, U.S. SMALL BUSINESS ADMINISTRATION
CHAIR, LEGISLATION COMMITTEE, COUNCIL OF THE INPSECTORS GENERAL FOR INTEGRITY AND EFFICIENCY

BEFORE THE

SUBCOMMITTEE ON EFFICIENCY AND EFFECTIVENESS OF FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
U.S. SENATE

"STRENGTHENING GOVERNMENT OVERSIGHT: EXAMINING THE ROLES AND EFFECTIVENESS OF OVERSIGHT POSITIONS WITHIN THE FEDERAL WORKFORCE"

NOVEMBER 19, 2013

Good afternoon, Chairman Tester, Ranking Member Portman, and Members of the Committee. On behalf of the Chair of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE), I am honored to represent the Federal Inspector General (IG) community this morning to discuss our work and recent accomplishments, and some of the challenges we face in carrying out oversight duties. I currently serve as the Chair of CIGIE's Legislation Committee.

Let me begin by thanking this Subcommittee, on behalf of the IG community, for your continuing support of our mission and your interest in our work. This support is longstanding and bipartisan, and we are truly grateful.

I am pleased to report to this Subcommittee that the Inspector General Reform Act of 2008 (or IG Reform Act) is working as intended. CIGIE serves a leadership role and is the core of the IG community. Together, the work of the IG community resulted in significant improvements to the economy and efficiency of programs Government-wide, with potential savings totaling approximately $46.3 billion. With the IG community's aggregate FY 2012 budget of approximately $2.7 billion, these potential savings represent about a $17 return on every dollar invested in the OIGs.

Notwithstanding these results, OIGs do face certain challenges as they work to improve the efficiency and effectiveness of government programs. Our principal challenges pertain to

independence concerns and to timely access to information. In recent years, CIGIE has been advocating for additional tools to alleviate these challenges and enhance our ability to do our jobs for the taxpayers.

CIGIE feels strongly that OIGs should be exempted from the Computer Matching and Privacy Protection Act relative to using electronic means to identify those who improperly receive Federal assistance and/or payments and subsequently, seek removal from the program and/or recoveries after verification and applicable due process. This would improve program efficiency and enables the Government to focus resources on eligible applicants.

Similarly, CIGIE has recommended that the Paperwork Reduction Act (PRA) be amended to exempt Federal IG offices from its requirements. The PRA requires that information collections, such as OIG surveys, be subject to approval from a "senior official" of the agency and then from OMB. While the 1995 PRA Amendments specifically exempted independent regulatory agencies from these requirements, and continues to exempt the Government Accountability Office, they were silent on the question of application to IGs. These exemptions would enhance the independence of IGs and remove lengthy processes that are better aligned with the role of Government interactions with the public, than oversight of the Government entity by the OIG.

The IG community has been hit especially hard by the uncertainty in the budget process and cuts to operating budgets. OIGs by nature are comprised principally of personnel, and their budgets are dedicated to funding the same. A recent survey of the IG community by the Association of Government Accountants found that more than two-thirds of the IGs interviewed identified budget resources as a top challenge. Many offices reported undertaking hiring restrictions and limiting new investments to operate under current budget levels. To highlight this finding, in my office, we have an approximate 17 percent vacancy rate due to an ongoing hiring freeze.

As an IG, I am grateful that IGs across the Government have a voice through CIGIE and have access to training and other resources that did not exist prior to the IG Reform Act. The IG Reform Act established CIGIE to serve as a unified council of statutory Federal IGs, to carry out two key missions:

- address integrity, economy, and effectiveness issues that transcend individual Government agencies; and
- increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

CIGIE's members currently include 72 IGs from the executive and legislative branches of Government, as well as 6 senior administration officials with related portfolios and responsibilities.

In accordance with CIGIE's primary mission, over the past several years the IG community has identified and addressed a number of issues that transcend individual agencies. CIGIE has issued reports on such topics as cybersecurity, suspension and debarment, the use of new media, the effectiveness of the Chief Financial Officers Act of 1990, disaster preparedness programs,

international trade and competitiveness, IG hotline operations and whistleblower protections, the Federal Audit Clearinghouse, and IG oversight of the American Recovery and Reinvestment Act of 2009. These reports and others are available on CIGIE's website at www.ignet.gov.

CIGIE's training and professional development mission is addressed through our Training Institute, which offers training to OIG audit, investigative, inspection and evaluation, leadership, and mission support personnel. Though the institute is still in a developmental phase, in FY 2012, the institute delivered 55 specialized training courses to 1,677 students, representing a 17 percent increase of students from the previous year.

CIGIE's standing committees are active bodies that are responsible for, among other things, developing professional standards that apply to overall OIG operations, as well as OIG audits, investigations, inspections, and evaluations. CIGIE, through its committees, also manages a peer review program of IG audit and investigation operations that evaluates OIG adherence to the professional standards. In FY 2012, CIGIE initiated a pilot program to peer review OIG inspection and evaluation activities on a voluntary basis. These programs play a critical role in advancing the professionalism of OIG operations and enhancing confidence in the quality of OIG products.

This concludes my testimony. Thank you again for inviting me to testify today before the Subcommittee about the role of CIGIE and challenges faced by the IG community. I would be pleased to address any questions you may have.

Office of the Inspector General
United States Department of Justice

Statement of Michael E. Horowitz
Inspector General, U.S. Department of Justice

before the

Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on the Efficiency and Effectiveness of Federal
Programs and the Federal Workforce

concerning

The Roles and Effectiveness of Oversight Positions
Within the Federal Workforce

November 19, 2013

Chairman Tester, Senator Portman, and Members of the Subcommittee:

Thank you for inviting me to testify at today's hearing. The need for strong and effective independent oversight over agency operations has never been more important. And that is what we do at the Office of the Inspector General (OIG) for the Department of Justice (Department or DOJ) – conduct thorough audits, investigations, evaluations, and reviews in order to assess whether the Department is operating effectively and efficiently, and to root out waste, fraud, abuse, mismanagement, and misconduct. The taxpayers rightly expect much from us, and I believe we have consistently demonstrated the value and importance of the work that we do. I am pleased to highlight for you some examples of the recent oversight work that the dedicated staff in our office has performed and the impact it has had, as well as to outline for you some of the obstacles that we have faced in conducting that independent oversight.

Examples of Recent DOJ OIG Oversight

During my 18 months as Inspector General, our office has issued numerous important reports. For example, our report on Operation Fast and Furious and Operation Wide Receiver detailed a pattern of serious failures in both the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) and the U.S. Attorney's Office's handling of the investigations, as well as in the Department's response to Congressional inquiries about those flawed operations. Our interim report on the Department's handling of known or suspected terrorists in the federal Witness Security (WITSEC) Program detailed significant information sharing failures that may have enabled WITSEC Program participants who were on the Transportation Security Administration's No Fly list to fly on commercial airplanes using their new government-issued identities. Another recent OIG report examined the ATF's use of income-generating undercover operations and found a serious lack of oversight by ATF, the misuse of proceeds, and failures to properly account for cigarettes with a retail value of over $100 million and other assets purchased during the investigations.

We also have conducted, and continue to conduct, extensive oversight of the Department's use of its various national security-related authorities, including those under the Patriot Act. For example, we issued reports on the Federal Bureau of Investigation's (FBI) activities under Section 702 of the *Foreign Intelligence Surveillance Act (FISA) Amendments Act*; the Department's coordination of its efforts to disrupt terrorist financing; and the FBI's Foreign Terrorist Tracking Task Force's sharing of information. Additionally, we expect to issue in the near future reviews on the FBI's use of National Security Letters (NSL), Section 215 Orders, and Pen Register and Trap-and-Trace Authorities under FISA, and the management of terrorist watchlist nominations. Additionally, we recently reviewed the Department's domestic use of drones or

unmanned aircraft systems (UAS), the privacy implications of the use of UAS, and the Department's support and provision of UAS to local law enforcement agencies and non-profit organizations.

We also have completed many reports that did not necessarily make headlines but will help make the Department's operations more effective and efficient and result in important savings of taxpayer dollars. In the past 12 months, we issued 90 reports, which included annual financial statement audits, information security audits, and audits of grant recipients. During this same period, our Investigations Division received more than 12,000 complaints, had dozens of arrests and convictions resulting from corruption and fraud cases, and investigated allegations that resulted in more than 250 administrative actions against Department employees.

The independent oversight conducted by our office routinely produces measureable benefits for the taxpayer. Over the past 10 fiscal years, our office has identified over $900 million in questioned costs – more than the OIG's budget during the same period. In addition, we have identified nearly $250 million in taxpayer funds that could have been put to better use by the Department, and our criminal and administrative investigations have resulted in more than $118 million in civil, criminal, and non-judicial fines, assessments, restitution, and other recoveries over that same period.

Moreover, when we issue our audits and reviews, we regularly make recommendations to the Department on how it can reduce costs and improve its programs. While many of our recommendations have already been implemented and resulted in improvements at the Department, hundreds of OIG recommendations remain open. The Department must redouble its efforts to adopt and implement these recommendations.

I am particularly proud of having instituted the first-ever DOJ OIG whistleblower ombudsperson program, and I am committed to ensuring that whistleblowers in the Department can step forward and report fraud, waste, abuse, and misconduct without retaliation. I have seen first-hand the important role that whistleblowers play in advancing the OIG's mission to address wasteful spending and improve the Department's operations, and whistleblowers should never suffer reprisal for coming forward with what they reasonably believe to be evidence of wrongdoing. The whistleblower ombudsperson program recently prepared a video entitled "Reporting Wrongdoing: Whistleblowers and their Rights and Protections," which was used in training programs for all OIG employees, and the OIG is working to provide this important training to other Department components. Our efforts were recognized this fall when the U.S. Office of Special Counsel certified that our Office had met its statutory obligation to inform its workforce about the rights and remedies available under the Whistleblower Protection Act. We will continue to do all we can to ensure that we are responsive to complaints that

we receive, and to respond appropriately to allegations of retaliation against whistleblowers.

Challenges Facing the DOJ OIG

Our audits, reviews, and investigations exemplify the professionalism and determination of the OIG staff to conduct thorough oversight, even in an environment of uncertain resources and occasional impediments. I would like to briefly highlight for you some of the challenges we face in conducting that oversight.

Impact of Sequestration

As we all know, these are difficult budgetary times across the government, including for Inspectors General. Even under these challenging resource constraints, we have produced quality reports and continued to conduct thorough investigations.

Yet, sequestration is having a real impact on Inspectors General. Because the great majority of our budget supports salaries for personnel, the substantial budget reduction for our office in FY 2013 combined with the uncertain budget situation for FY 2014 has caused me to lower our staffing ceilings by approximately 40 FTE since my arrival in April 2012, representing approximately 8 percent of our staff. While we always strive to improve our productivity and efficiency, further reductions in personnel will inevitably require us to reduce the number of audits, investigations, and reviews that we conduct, and may impact how we proceed with the audits, investigations, and reviews that we are able to perform.

In addition to reducing our staff through attrition, we also have implemented a number of significant cutbacks that have had an impact on how we perform our work. For example, our need to drastically curtail travel costs required us, in some instances, to limit the scope of reviews, to put entire audits on hold, and to emphasize the importance of cost considerations in selecting audits at the expense of substantive considerations. It has long been our belief that an on-site inspection is necessary in most cases in order to achieve the highest quality of review that is properly expected of an OIG. These visits allow our auditors and inspectors to better gauge how processes are conducted and, in turn, to potentially offer the most useful recommendations for improvement. Yet, our ability to conduct these on-site inspections has been necessarily limited due to budget cutbacks.

Despite these financial challenges, I am confident that the dedicated professionals in our office and in all OIGs will continue to provide extraordinary service to the American public.

Access to Documents Relevant to OIG Reviews

For any OIG to conduct effective oversight, it must have complete and timely access to all records in the agency's possession that the OIG deems relevant to its review. This is the principle codified in Section 6(a) of the Inspector General Act, which authorizes Inspectors General "to have access to all records, reports, audits, reviews, documents, papers, recommendations or other material available to the applicable establishment which relates to programs and operations with respect to which that Inspector General has responsibilities under this Act." This principle is both simple and important, because refusing, restricting, or delaying an OIG's access to documents may lead to incomplete, inaccurate, or significantly delayed findings or recommendations, which in turn may prevent the agency from correcting serious problems in a timely manner.

Most of our audits and reviews are conducted with full and complete cooperation from Department components, and with timely production of material. However, there have been occasions when our office has had issues arise with access to certain records due to the Department's view that access was limited by other laws. For example, issues arose in our review of Operation Fast and Furious regarding our access to grand jury and wiretap information that was directly relevant to our review, and to wiretap information that was directly related to our ongoing review of the Department's use of Material Witness Warrants. Ultimately, in each instance, the Attorney General and the Deputy Attorney General provided the OIG with written permission to receive the materials because they concluded that the two reviews were of assistance to them. While the Attorney General and Deputy Attorney General have made it clear that they will continue to provide the OIG with the necessary authorizations to enable us to obtain records in future reviews, requiring an Inspector General to obtain a memorandum from Department leadership in order to be allowed to review critical documents in the Department's possession impairs our independence and conflicts with the core principles of the Inspector General Act.

We have had similar issues regarding our access to some other categories of documents, including FISA information, which is obviously critical for us to review in connection with our national security reviews. And I understand that several Inspectors General at other federal agencies have had similar issues regarding access to records within their agencies. Although our office has not yet had an instance where materials were ultimately withheld from us that were necessary to complete our review, we remain concerned about the legal questions that have been raised and the potential impact of these issues on our future reviews. Moreover, issues such as these have, at times, delayed our access to documents that were essential to conducting our reviews, thereby substantially impacting the time required to complete the review.

My view, and I believe the view of my colleagues in the Inspector General community, is straightforward and follows from what is explicitly stated in the Inspector General Act: An Inspector General should be given prompt access to all relevant documents within the possession of the agency it is overseeing. For a review to be truly independent, an Inspector General should not be required to obtain the approval or authorization of the leadership of the agency in order to gain access to certain agency records, and the determination about what records are relevant to a review should be made by the Inspector General and not by the component head or agency leadership. Such complete access to information is a cornerstone of effective independent oversight.

Limitations on the DOJ OIG's Jurisdiction

Let me conclude by briefly turning to a limitation on our oversight ability that is unique to my OIG: unlike OIGs throughout the federal government, our office does not have authority to investigate all allegations of misconduct within the agency we oversee. While we have jurisdiction to review alleged misconduct by non-lawyers in the Department, under Section 8E of the Inspector General Act, we do not have jurisdiction over alleged misconduct committed by Department attorneys when they act in their capacity as lawyers – namely, when they are litigating, investigating, or providing legal advice. In those instances, the Inspector General Act grants exclusive investigative authority to the Department's Office of Professional Responsibility (OPR). As a result, these types of misconduct allegations against Department lawyers, including any that may be made against the most senior Department lawyers (including those in Departmental leadership positions), are handled differently than those made against agents or other Department employees. The OIG has long questioned this distinction between the treatment of misconduct by attorneys acting in their legal capacity and misconduct by others, and this disciplinary system cannot help but have a detrimental effect on the public's confidence in the Department's ability to review misconduct by its own attorneys.

This jurisdictional limitation on our office is a vestige of the fact that OPR pre-existed the creation by Congress in 1988 of the OIG for the Department of Justice, resulting in the statutory carve-out on our jurisdiction. The Department has repeatedly taken the position that because OPR has specialized expertise in examining professional conduct issues involving Department lawyers, OPR should handle professional misconduct allegations against Department attorneys. Whatever merit such an argument may have had in 1988 when the OIG was established by Congress, it is surely long outdated. Over the past 25 years, our office has shown itself to be capable of fair and independent oversight of the Department, including investigating misconduct allegations against its law enforcement agents. Indeed, a similar argument was made many years ago by those who tried to forestall OIG oversight of alleged FBI agent misconduct. This argument against OIG oversight of the FBI was rejected, and as we have demonstrated through our

hundreds of reviews involving Department law enforcement matters since then, including our recent Fast and Furious review, our office has the means and expertise to handle the most sophisticated legal and factual issues thoroughly, effectively, and fairly. Moreover, other OIGs across the federal government handle misconduct allegations against lawyers in their agencies, and they have demonstrated that OIGs are fully capable of dealing with such matters. Seen in this context, the carve-out for OPR from the OIG's oversight jurisdiction is best understood as an unnecessary historical artifact.

Eliminating the jurisdictional carve-out for OPR in the Inspector General Act would ensure the ability of the OIG to fully review and, when appropriate, investigate allegations of misconduct of all Department employees. The OIG's statutory and operational independence from the Department ensures that the investigation of allegations of misconduct against Department employees occur through a transparent and publically accountable process. Unlike the head of OPR, who is appointed by the Attorney General and can be removed by the Attorney General, the Inspector General is a Senate confirmed appointee who can only be removed by the President after notification to Congress, and the Inspector General has reporting obligations to both the Attorney General and Congress. Additionally, the OIG's strong record of transparency is vital to ensuring the Department's accountability and enhancing public confidence in the Department's operations. Giving the OIG the ability to exercise jurisdiction in these cases, just as we do in matters involving non-attorneys throughout the Department, would enhance the public's faith in the outcomes of these important investigations and provide our office with the same authority as other Inspectors General.

This concludes my prepared statement, and I would be pleased to answer any questions that you may have.

Testimony of the Honorable Carolyn N. Lerner, Special Counsel
U.S. Office of Special Counsel

U.S. Senate Committee on Homeland Security and Governmental Affairs
Subcommittee on the Efficiency and Effectiveness
of Federal Programs and the Federal Workforce

"Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions within the Federal Workforce"

November 19, 2013, 2:30 P.M.

Chairman Tester, Ranking Member Portman, and Members of the Subcommittee:

Thank you for the opportunity to testify today about the U.S. Office of Special Counsel (OSC). OSC is an independent investigative and prosecutorial federal agency. We protect the merit system for over 2.1 million civilian federal employees in four distinct mission areas. OSC protects federal workers from "prohibited personnel practices," especially retaliation for whistleblowing. We provide a safe and secure channel for whistleblowers to report waste, fraud, abuse, and health and safety issues. We enforce the Hatch Act, keeping the federal workplace free from improper partisan politics. Finally, OSC enforces the Uniformed Services Employment and Reemployment Rights Act (USERRA).

We fulfill these important roles with a staff of approximately 110 employees – and the smallest budget of any federal law enforcement agency. I am pleased to report that our dedicated staff is performing more efficiently and effectively than at any point in OSC's 35-year history.

However, our capacity for improving government is limited by extreme resource challenges. In the past two years, OSC's caseloads skyrocketed to historic levels. In addition, Congress imposed important new mandates on OSC with passage of the "Whistleblower Protection Enhancement Act of 2012." Despite these increases in our workload, OSC's already flat budget took a dramatic hit with sequestration, causing workforce reductions.

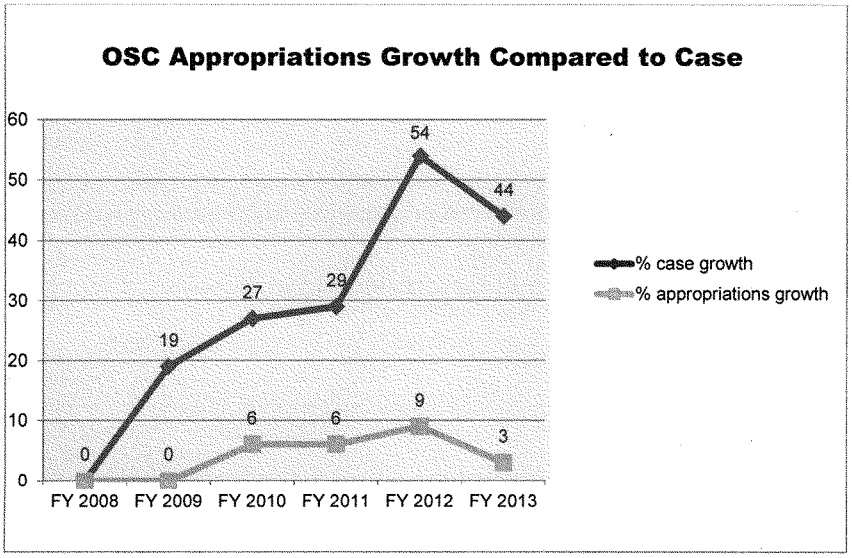
The simple mathematics of historically-high case levels and a shrinking budget poses the biggest challenge to OSC in realizing our oversight potential. The good news is that Congress and the administration recognize that the status quo is not sustainable. The President's Fiscal Year 2014 budget request for OSC provides a necessary increase of approximately $1.7 million, which both the House and Senate Appropriations Committees approved. While we are currently operating, like most agencies, under a continuing resolution, I am hopeful that final spending bills for 2014 will include this modest increase.

With that overview, I want to provide more detail on OSC's track record over the last two years and conclude by briefly noting issues beyond resource challenges that may pose obstacles to OSC.

OSC Accomplishments with Limited Resources and Staff

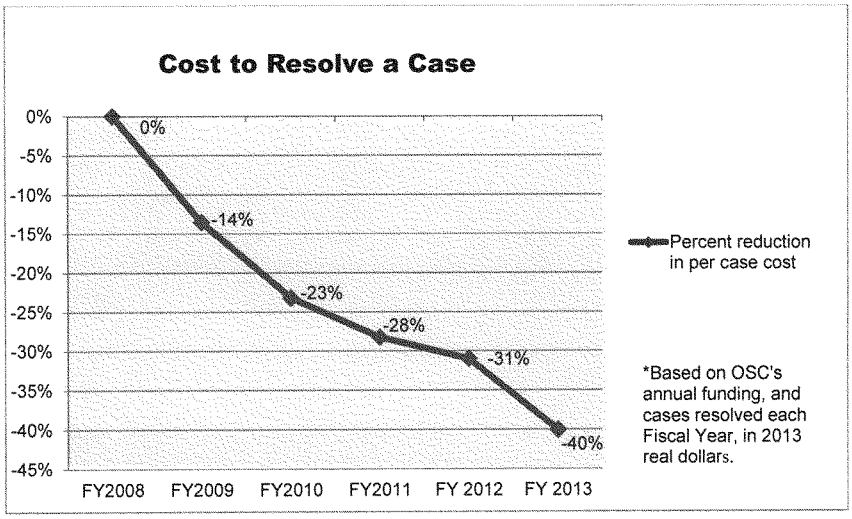
The last two fiscal years (FY2012 and FY2013) have been a record-setting period for OSC. By nearly every statistical measure, OSC achieved the most positive results in its history. These successes result in greater confidence in OSC's ability to perform its good government mission. However, such confidence can be a double-edged sword, as it directly correlates to our increased caseload.

To illustrate, cases increased by 50% in five years, with the sharpest increase over the last two. During this period, funding levels actually decreased in real terms, considering inflation, automatic pay adjustments, and other mandatory expenses.



In addition to receiving more cases, OSC is processing them more efficiently and effectively. For example, in FY2008, OSC completed a total of 2,875 cases. In FY2013, just five years later, OSC resolved 4,808 cases, nearly doubling our productivity. Completing cases quickly benefits employees and enables agencies to manage their workforce with less disruption and uncertainty.

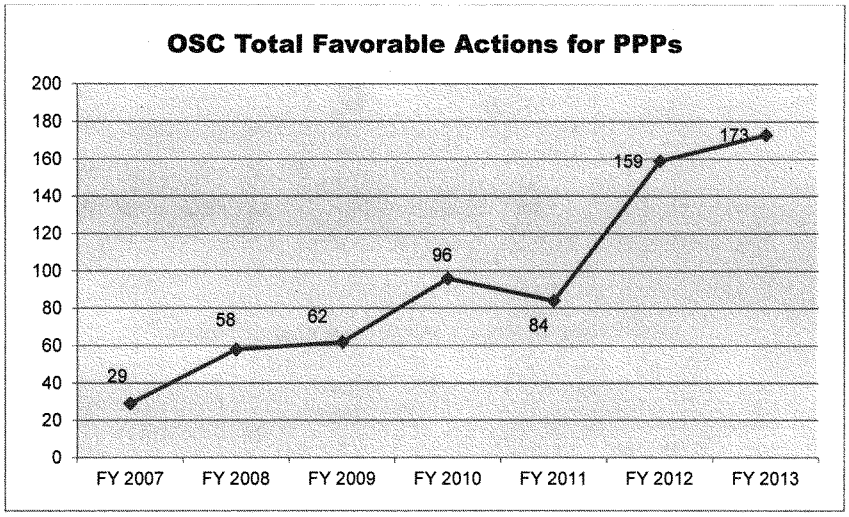
OSC's increased efficiency helps us manage the growing caseload, and translates into real savings. OSC's cost to resolve a case dropped by 40% in the last 5 years, a decrease of over $2,640 per case. Stated simply, we're making every dollar count.



Our increased efficiency has not compromised OSC's effectiveness. In fact, when evaluating the most important statistic for OSC – the number of favorable actions on behalf of whistleblowers and the merit system – we are again setting records. We're not just closing cases, we're getting more relief than ever before for whistleblowers. Favorable actions include the relief that OSC secures for employees who are the victims of retaliation, such as back pay, reinstatement, or reassignment to a non-retaliatory environment. They include disciplinary actions taken against employees who engage in retaliation or other prohibited conduct. And favorable actions also include cases where we work with agencies to implement systemic reforms to prevent problems from recurring.

In FY2012, the first full year of my tenure, our staff achieved an 89% increase in favorable actions from the prior fiscal year. This was a 175% increase from five years ago. FY2012's total of 159 favorable actions, or "victories" for whistleblowers and the merit system, exceeded any previous year in the agency's history. We set an extremely high bar in FY2012, and then surpassed it in FY2013. The total number of favorable actions rose again in FY2013 – to 173. This is an astonishing total, considering only 29 favorable actions were achieved in 2007.

It is a testament to the hard work of our dedicated career staff, who have endured furloughs and increased caseloads while managing to improve productivity and outcomes in all measures.



These numbers don't tell the whole story. Statistics cannot capture the true impact and value of OSC's work. Our efforts to support whistleblowers often stop the immediate problem and spark reforms that prevent wasteful, inefficient, or unsafe practices.

For example, OSC recently issued a report detailing serious overtime abuse by Department of Homeland Security employees. Improper claims of Administratively Uncontrollable Overtime, or AUO, cost the government up to $9 million annually at six DHS offices identified by whistleblowers in OSC cases. The annual cost of AUO abuse nationwide is likely to reach tens of millions of dollars, according to the whistleblowers. And this estimate excludes overtime claims by agents in the field – those whose need for AUO would seem to be most justified. It is my sincere hope that OSC's role in highlighting this gross waste of scarce government funds will assist the Subcommittee in its efforts to reform the DHS overtime system, and I applaud you for your efforts in this area.

In the past year, OSC also worked with whistleblowers at the VA Medical Center in Jackson, Mississippi. Physicians and other employees raised concerns about unlawful prescriptions of narcotics, chronic understaffing of the Primary Care Unit, unsterile medical equipment, and other threats to Veterans at the facility. OSC's efforts resulted in greater oversight of the Jackson VAMC by the administration and Congress, and we are continuing to work with whistleblowers to identify and address similar problems throughout the VA system.

In the last two years, OSC also successfully carried out its expanded role to protect the rights of returning service members under USERRA. Under a three-year pilot program mandated by Congress, OSC is investigating half of all federal sector USERRA claims, while the Department

of Labor continues to investigate the other half. OSC is using an effective and low-cost approach to resolving USERRA cases through Alternative Dispute Resolution. OSC achieved a 100% success rate in resolving USERRA claims referred to mediation.

In one recent USERRA case, a member of the Air Force Reserves worked with the Department of Energy in New Mexico. Upon her return from active duty, the Department refused to promote her, after initially promising that it would. Management officials cited her absence for military service as the reason. OSC investigated and informed the agency of its obligations under USERRA. The Department of Energy then gave the reservist a retroactive promotion with corresponding back pay and reassigned her within the agency, enabling her to get the experience and training necessary for further promotion.

Among the favorable actions OSC received for whistleblowers was a case originating in Syracuse, NY. Two whistleblowers at the Transportation Security Administration blew the whistle on misuse of a government vehicle, misuse of financial rewards, and a hostile work environment at the Syracuse Hancock International Airport. The whistleblowers were retaliated against after making these disclosures, and both received full corrective action after OSC's investigation. One of the whistleblowers told a Syracuse newspaper, "We were a little frustrated, like no one's going to help us . . . And (OSC) hung in there and did good things for us." The whistleblower specifically noted the work of OSC Attorney Clarissa Pinherio, who worked on the case for three years and ultimately was able to negotiate relief for the employees.

Finally, during 2012, OSC successfully enforced the Hatch Act during a difficult presidential election year, including finding a sitting cabinet secretary in violation of the Hatch Act for the first time in the Act's history.

Whistleblower Protection Enhancement Act (P.L. 112-199) Will Further Increase OSC's Caseloads

OSC is also in the process of implementing the first major reform to the federal whistleblower law in 20 years. The Whistleblower Protection Enhancement Act (WPEA) was signed into law on November 28, 2012. The landmark reform was supported by a broad, bipartisan coalition in Congress, with strong support from good government and taxpayer protection organizations. OSC is the primary agency responsible for implementing this good government reform and already has seen a significant increase in claims. During the first quarter of FY2013, OSC experienced the highest number of quarterly filings in the agency's 35-year history.

The Congressional Budget Office conservatively estimated that OSC would need an additional $1 million annually to successfully implement the WPEA. However, under sequestration, OSC's resources have been reduced by $1 million since enactment of the WPEA, significantly impeding OSC's ability to carry out the law's good government mandates. While we shifted additional staff to our Investigation and Prosecution Division to help manage the workload, our budget to pay for basic investigative expenses – such as transcription services – is inadequate. Similarly, we cannot afford to conduct on site investigations in whistleblower reprisal cases and other matters, except for the most extraordinary circumstances.

The WPEA's mandates include: a significant expansion of OSC's jurisdiction; a requirement to conduct investigations in hundreds of whistleblower cases that previously would have been dismissed; a direction from Congress to initiate more formal litigation and disciplinary actions against agency managers; and training requirements for all other government agencies. The WPEA also provides OSC with the authority to file amicus briefs in federal court cases that involve whistleblower protection issues. OSC exercised this new authority for the first time in the case of *Kaplan v. Conyers*, arguing that the Federal Circuit Court of Appeals' decision threatened to undermine the enhanced whistleblower protections passed by Congress.

Other Challenges

In conclusion, I would like to flag two additional areas that the Subcommittee may want to consider as it examines possible efforts to strengthen oversight positions in the government.

First, the Federal Circuit's decision in *Kaplan v. Conyers* poses a significant threat to whistleblower protections for hundreds of thousands of federal employees in sensitive positions and may chill civil servants from blowing the whistle. I understand that the Subcommittee will hold a hearing to examine the impact of *Conyers*, and I applaud your efforts to better understand this important issue.

While the *Conyers* Court did not specifically address the applicability of the decision to whistleblower and other prohibited personnel practice cases, it may be helpful for Congress to clarify that OSC and the MSPB maintain jurisdiction over employee claims of retaliation and other prohibited conduct, even where an adverse employment action is based on the employee's eligibility to hold a sensitive position. It may also be helpful for Congress to track the number of adverse actions taken because an employee is deemed ineligible to hold a sensitive position, rather than the traditional bases for punishment – employee conduct or performance. If the number of actions based on eligibility begins to trend upward, it would indicate that agencies are more actively utilizing the authority provided by *Conyers*, and my concerns about the impact on the merit system and due process rights for federal workers would increase.

Second, OSC has not been formally reauthorized since 2007. While this does not prevent OSC from receiving appropriations, reauthorization provides Congress with an opportunity to evaluate OSC's authorities and responsibilities and make any necessary adjustments. In light of our steadily increasing workload, Congress may want to consider the onerous procedural requirements imposed on OSC in all prohibited personnel practice cases as a possible area for revision. Additionally, there is no statute of limitations for filing a prohibited personnel practice complaint with OSC. Congress may want to consider whether a reasonable time limit for filing a complaint with OSC is appropriate. Finally, OSC's authority to compel the production of documents in whistleblower disclosure cases could be clarified, and the mechanism for enforcing OSC subpoenas against federal entities should be updated and streamlined.

Investing in OSC is one of the most cost-effective methods of promoting good government and preventing violations of merit system laws. I thank you for the opportunity to testify today, and I look forward to your questions.

WRITTEN TESTIMONY

of

KAREN NEUMAN

CHIEF PRIVACY OFFICER

DEPARTMENT OF HOMELAND SECURITY

Before the

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUBCOMMITTEE ON THE EFFICIENCY AND EFFECTIVENESS OF

FEDERAL PROGRAMS AND THE FEDERAL WORKFORCE

November 19, 2013

Good morning Chairman Tester, Ranking Member Portman, and Members of the Committee. I appreciate the opportunity to appear before you today to discuss the role of the Department of Homeland Security (DHS) Privacy Office and how our oversight responsibilities complement our policy and compliance functions to ensure privacy rights are protected as the Department carries out its various, critical missions.

As you know, Section 222 of the Homeland Security Act of 2002 established the Chief Privacy Officer as the first statutorily mandated privacy official in the federal government. Under the Homeland Security Act, the Privacy Office is charged with ensuring the Department's use of technology sustains and does not erode privacy protections relating to the use, collection, and disclosure of personally identifiable information (PII). In this effort I am assisted by highly qualified privacy professionals who also work to ensure that DHS's collection and use of information is in full compliance with fair information practice principles (FIPPs).

It is important to note that the Privacy Office is not a pure oversight office. We manage a portfolio of statutory responsibilities that includes oversight in addition to policy and compliance functions. Our challenge, therefore, is to understand how oversight responsibilities impact our compliance and policy functions, and blend them into a coordinated mission set that the Privacy Office can implement in support of privacy interests for activities across the Department.

The Privacy Office is a Policy Office

Section 222 of the Homeland Security Act established the Chief Privacy Officer as the principal policy advisor to the Secretary of Homeland Security for privacy matters. This highly specialized

role is a separate and distinct role from the Department's other policy-making functions. In this capacity, the Privacy Office has issued a number of Department-wide policies including the DHS-wide Management Directive on Privacy Policy and Compliance as well as policies on the use of social security numbers and social media at DHS, loss or unauthorized use or disclosure of PII, and protection of terrorism-related information shared within the Information Sharing Environment.

In addition to crafting privacy policy guidance, the Privacy Office focuses on operationalizing privacy at DHS by building a first-rate privacy compliance team and process designed to ensure that program managers and frontline personnel understand how their use of data impacts privacy and that systems are designed and operate in full compliance with all applicable laws. We work closely with components and offices—at each stage of program or system development—to "bake privacy in" by implementing the FIPPs as set forth in DHS Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security. The Privacy Impact Assessment (PIA) has also become a powerful tool for accomplishing this mandate.

The PIA as a Document and a Process

A PIA is a document that serves a very important function by providing transparency into DHS operations and describing the ways in which privacy has been built into DHS information technology systems, programs, initiatives, and rulemakings. DHS has published more than 500 PIAs on its website where interested citizens and organizations can learn about how information is collected, used, and shared by the Department.

The PIA is also a process. To conduct a PIA, the Privacy Office partners with mission personnel across the Department, component privacy staff, and other stakeholders including the Office of the General Counsel (OGC), the Office for Civil Rights and Civil Liberties (CRCL), the Office of Policy, and others. Under the direction of the Privacy Office, key organizations work together at the earliest stages of system development to identify potential privacy risks and to mitigate them, before they harm individual privacy. The evaluation and mitigation process is repeated and refined at each stage of development, as uses of information and technological capabilities evolve.

The result of this process is the written PIA document, which reflects our involvement even in the early development of the Department's sensitive programs, systems, or other initiatives. Indeed, we believe that—for the majority of our work—privacy is best protected when we provide advice on privacy requirements and policy at every stage in a program or system's life cycle.

The Privacy Office is an Oversight Office

In addition to its role as a policy office, the Privacy Office serves an important oversight role at DHS as part of a layered approach to oversight that includes the component privacy officers at DHS and the DHS OIG, GAO, Congress, the Office of Management and Budget (OMB), and the Privacy and Civil Liberties Oversight Board (PCLOB), and the American public, who are an important part of the Nation's privacy dialogue and informed, in part, through our published PIAs and other efforts to enhance transparency.

In 2007, Congress amended Section 222 of the Homeland Security Act to include additional oversight authorities, including: the power to investigate Department programs and operations; to issue subpoenas to non-federal entities; and to administer oaths, affirmations, and affidavits necessary to conduct investigations. In 2012, the Privacy Office fully implemented these changes by creating the Privacy Oversight Team, responsible for Privacy Compliance Reviews (PCRs), privacy investigations, privacy incident response, and privacy complaint handling and redress. To accomplish their mission, the Oversight Team has forged close working relationships with other oversight offices like the OIG and redress offices like DHS Travelers Redress Inquiry Program (TRIP).

In the past 12 months, the Privacy Oversight Team conducted six PCRs, which are a hybrid of investigative activities and collaborative decision-making. They are designed to improve programs' ability to comply with the assurances to protect privacy reflected in PIAs, Privacy Act System of Record Notices, which are published in the Federal Register, and Information Sharing Access Agreements, which establish terms and conditions—including privacy protections—for receiving PII from DHS. The Privacy Office collaboratively undertakes PCRs of high-profile privacy-sensitive programs and partners with programs to identify and rectify any compliance gaps and design mutually-acceptable paths to improvement. Examples of programs examined include the Department's use of social media for situational awareness, DHS's participation in the Nationwide Suspicious Activity Reporting Initiative, and the Department's implementation of the 2011 U.S.-EU Passenger Name Record (PNR) Agreement. These and other PCRs may

result in recommendations for additional privacy protections, updates to existing privacy compliance documentation, and presentations of lessons learned.

When necessary, and as authorized by Congress, the Privacy Office has conducted a number of investigations in the event of significant non-compliance with Departmental privacy policy. For example, one investigation concerned a privacy incident involving loss of an unencrypted flash drive with financial audit data that contained Sensitive PII. In February 2011, the Privacy Office published a report with detailed findings, setting forth proactive recommendations to prevent and mitigate similar privacy incidents.

The Privacy Office also conducts a number of rolling oversight reviews. These include:

- Intelligence Products Review – The Privacy Office provides same-day review of finished intelligence products disseminated to fusion centers and threat briefings given to the private sector.
- Automated Targeting Rules Review – The Privacy Office, along with CRCL and OGC, conduct quarterly reviews of scenario-based counterterrorism automated targeting rules that DHS uses to prioritize passenger screening efforts at airports and at the U.S. border.
- Quarterly Metrics Reporting Review – As part of the information sharing agreements between DHS and the National Counterterrorism Center (NCTC), the two organizations hold quarterly meetings as required by the agreements. Once again, the Privacy Office teams with CRCL, OGC, and representatives from the Office of Intelligence and Analysis and component data stewards to review reporting metrics stemming from NCTC's access to and use of DHS data.

Privacy Office Oversight Part of a Layered Approach to Oversight

The DHS Privacy Office is able to manage the dual role of being both policy advisor and oversight office because of our collaboration with the DHS OIG and GAO. Both offices have built exceptional audit teams to examine privacy issues and the DHS Privacy Office is a frequent participant in these audits, which reinforce our efforts to protect privacy and as a driver of best-practices when our own actions are reviewed.

Component Privacy Officers at DHS serve a vital role within their component's programs and initiatives, greatly enhancing the effort to bake privacy in across the Department. These officials, implementing policy developed by the Privacy Office and ensuring compliance, serve as a key driver in helping systems, programs, initiatives, and rulemakings address privacy as part of their development. These Component Privacy Officers also enhance the oversight activities by participating in PCRs, privacy investigations, and incident responses. They are an important source of recommending programs that the DHS Privacy Office may wish to review.

In addition, OMB provides oversight on privacy issues. For example, OMB reviews our Federal Information Security Management Act (FISMA) privacy scores that we submit annually, along with reports on our activities required every quarter under Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*.

We are also pleased with the reconstitution of the Privacy and Civil Liberties Oversight Board (PCLOB), which is charged with, among other things, analyzing and reviewing actions the

executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties. We interact and consult regularly with the PCLOB as part of these efforts.

Through these efforts and others we hope to provide the public with a greater understanding of privacy risks and the steps we take at DHS to mitigate those risks.

Conclusion

Thank you for the opportunity to discuss the DHS Privacy Office and our privacy oversight role. Our unique challenge is to ensure our oversight activities work in harmony with our compliance and policy functions. This effort is supported by the existence of and partnership with the Department's component privacy officers, oversight offices like the DHS OIG and GAO, as well as our relationship with Congress, OMB, and the PCLOB. I look forward to answering your questions.

"Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions within the Federal Workforce"

Statement of Wendy Ginsberg, Ph.D.

Analyst in American National Government

Congressional Research Service

Before the

Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce

November 19, 2013

Chairman Tester, Ranking Member Portman, and distinguished Members of the Subcommittee, thank you for opportunity to testify before you today on Obama Administration transparency initiatives and their effect on federal oversight.

An Overview of Congressional Oversight

Oversight lacks a precise or consensus definition, and, in fact, is not mentioned specifically in the Constitution. Yet, oversight plays a key role in ensuring that our nation's laws are faithfully executed. Oversight is an implied constitutional power of Congress. On Capitol Hill, it is performed in various ways by different committees and individual Members.

One objective of oversight is to hold executive officials accountable for the execution and implementation of authorities that have been assigned or delegated to them.[1] Oversight is integral to Congress's legislative authority. It can ensure executive branch compliance with legislative intent, evaluate program performance, find efficiencies, investigate allegations of abuse or wrongdoing, assess an agency's capacity to execute its mission, ensure that executive branch policies reflect the public interest, and increase public confidence in federal programs and agencies.[2] Oversight can help ensure that the federal government is operating economically, efficiently, and effectively. Determining the appropriate quantity and quality of oversight, however, is not a simple task.

Oversight has evolved as the size of and scope of the federal government has grown.[3] Various institutional and other developments have, in some cases, limited the ability of committees and lawmakers to carry out their oversight function in a continuous fashion. For example, there are simple time and resource limitations. Oversight can require a lot of time, a deep understanding of complicated issues, and—even when performed meticulously—may not culminate in an easily measurable outcome.[4] For example, what metrics could demonstrate the utility of oversight that increased public confidence in a particular program or agency?

To meet the challenge of overseeing the execution of laws in the executive branch, Congress employs a collection of oversight tools and techniques. Among these tools and techniques are hearings and investigations; legislatively authorizing, reauthorizing or abolishing an agency's duties; the appropriations

[1] For additional information on congressional oversight, generally, see CRS Report R41079, *Congressional Oversight: An Overview*, by Walter J. Oleszek.

[2] CRS Report RL30240, *Congressional Oversight Manual*, by Todd Garvey et al.

[3] For example, the so-called modern era of government has witnessed authorization for and creation of a "presidential branch" of government (the Office of Management and Budget, the National Security Council, and the like) and the establishment of many federal departments and agencies. From three departments in 1789 (State, Treasury, and War, renamed Defense in 1947), a dozen more have been added to the cabinet. The newest creation, in 2002, is the Department of Homeland Security (DHS). Formed from the merger of 22 separate executive branch units, it employees roughly 180,000 people. Other scholars have referred to the growth of the executive branch as "the administrative state." See Lawrence C. Dodd and Richard L. Schott, *Congress and the Administrative State* (New York: John Wiley and Sons, 1979).

[4] See, for example, the statement of a Senator in *Congress Speaks: A Survey of the 100th Congress* (Washington, DC: Center for Responsive Politics, 1988), p. 163.

process; reporting requirements;[5] the Senate confirmation process; general management laws that require program evaluation; [6] and casework.

Additionally, Congress has enacted transparency and information access laws that provide a foundation to leverage additional oversight. Among these authorities are:

- The Administrative Procedure Act (1946);
- The Inspector General Act (1978);
- The Freedom of Information Act (1966);
- The Government Performance and Results Act (1993); and
- The E-Government Act (2002).

Congress has authorized other institutions to conduct oversight, such as its creation of the Government Accountability Office and the enactment into law of 72 federal offices of inspectors general that are authorized to find waste, fraud, and abuse.

With this summary of the oversight process, let me discuss several transparency-related efforts in both the legislative and executive branches that feature technology in a prominent way. These laws and initiatives, arguably, have changed the way federal oversight has been and can be conducted.

I. Leveraging Technology to Enhance Data Accessibility and Increase Citizen Engagement

Advances in technology have opened up new avenues for public engagement with government. The public can watch congressional hearings in real time via committee websites, and they can contact Members and agencies through technologies that include email, Facebook, and Twitter. Access to federal databases and information has increased as a result of various legislative and executive branch initiatives. In many cases, access to accurate data can assist in making optimal policy decisions.[7] Access to information can also assist watchdog organizations, private and nonprofit entities, academics, and individual members of the public to assist in identifying issues of concern or importance to the federal government. Several examples illustrate this point.

Obama Administration's Open Government Initiative

One particular example of an executive branch effort that builds on Congress's foundational transparency laws is President Obama's Open Government Initiative. On his first full day in office President Obama

[5] For more information on reporting requirements, see CRS Report R42490, *Reexamination of Agency Reporting Requirements: Annual Process Under the GPRA Modernization Act of 2010 (GPRAMA)*, by Clinton T. Brass.

[6] For more on the authorities created by Congress to promote transparency and public oversight, see CRS Report R42817, *Government Transparency and Secrecy: An Examination of Meaning and Its Use in the Executive Branch*, by Wendy Ginsberg et al.

[7] *Government Transparency: Efforts to Improve Information on Federal Spending*, GAO-12-913T, July 18, 2012, pp. 11; and Partnership for Public Service, *From Data to Decisions II: Building an Analytics Culture*, October 2012, pp. 10-12.

outlined this initiative, which sought to make the federal government more transparent, participatory, and collaborative.

The Open Government Directive

On December 8, 2009, Peter R. Orszag, then-Director of the Office of Management and Budget (OMB), released the "Open Government Directive" memorandum, which included more detailed instructions for departments and agencies on how to "implement the principles of transparency, participation, and collaboration."[8] The memorandum required executive branch agencies to provide public, online access to "high-value" datasets that were previously unpublished.[9] Agencies were instructed to reduce their Freedom of Information Act (FOIA) backlogs by 10% per year, until they are eliminated.[10] In addition, the memorandum required each agency to designate a "high-level senior official to be accountable for the quality and objectivity of, and internal controls over, the Federal spending information" that agencies currently provide to government websites like *USAspending.gov* and *Recovery.gov*.[11] Each agency was also required to create an "open government plan ... that will describe how it will improve transparency and integrate public participation and collaboration into its activities."[12] The memorandum set a series of staggered deadlines for each department and agency to comply with the new requirements.

The directive aimed to implement the initiative's core values through four strategies:

1. Publish government information online.
2. Improve the quality of government information.
3. Create and institutionalize a culture of open government.
4. Create an enabling policy framework for open government.[13]

The Administration stated that the release of information and data would better enable the public to raise questions and keep agency performance in check—in effect, "crowdsourcing" oversight.[14]

---

[8] Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Open Government Directive*, December 8, 2009, at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

[9] An attachment to the memorandum provided a definition of what would qualify as a "high value data set," stating "[h]igh value information is information that can be used to increase agency accountability and responsiveness; improve public knowledge of the agency and its operations; further the core mission of the agency; create economic opportunity; or respond to need and demand as identified through public consultation." Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Open Government Directive*, December 8, 2009, Attachment, pp. 7-8.

[10] FOIA (5 U.S.C. § 552) provides the public presumed access to executive branch agency records. For more information on FOIA and particular categories of records that are exempted from public release, see CRS Report R41933, *The Freedom of Information Act (FOIA): Background and Policy Options for the 113th Congress*, by Wendy Ginsberg.

[11] Ibid., p. 3.

[12] Ibid., p. 4.

[13] Executive Office of the President, Office of Management and Budget, *Memorandum for the Heads of Executive Departments and Agencies: Open Government Directive*, Washington, DC, December 8, 2009.

[14] At a December 10, 2009, Senate Budget Committee Task Force on Government Performance hearing, both the federal CIO (then Vivek Kundra) and the federal CTO (then Aneesh Chopra) said that watch dog groups and members of the public would enforce agency accountability. U.S. Congress, Senate Committee on the Budget, Task Force on Government Performance, *Data-Driven Performance: Using Technology to Deliver Results*, 111th Congress, 1st session, December 10, 2009, at http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=budget121009&st=1005.

Private sector reviews of the open government initiative have suggested that executive branch agencies met the requirements with varying levels of performance. Some agencies released thousands of datasets and created user-friendly websites, while others released minor datasets and appeared to make little attempt to create websites that offered easy access to information.[15]

Fostering the Smart Disclosure of Federal Information

Perhaps to address some criticism of the Open Government Directive, in 2011, OMB released another transparency-related memorandum providing guidance to agencies on releasing datasets and information that are more useful to public consumers.

The OMB guidance, entitled "Informing Consumers through Smart Disclosure,"[16] defined smart disclosure as "the timely release of complex information and data in standardized, machine readable formats ... that enable consumers to make informed decisions." Smart disclosure, the memorandum continued, requires that data are accessible, machine readable,[17] standardized,[18] timely, adaptive to markets and innovation,[19] interoperable,[20] and protective of individuals' privacy.[21] Pursuant to the guidance, agencies were to determine "whether and how to best promote smart disclosure."[22] In May 2013, the federal Task Force on Smart Disclosure further detailed recommendations for implementation.[23] Among these recommendations were making federal agency data systems interoperable with other systems within and outside of individual agencies; ensuring that aggregated databases that are released to the public cannot be mined to inappropriately release sensitive information about individuals; and hosting

---

[15] One private entity's examination of the OGD was OMB Watch's (now known as The Center for Effective Government), "Leaders and Laggards in Agency Open Government Webpages," February 23, 2010, at http://www.foreffectivegov.org/node/10785/. OMB Watch also wrote a similarly mixed review follow-up assessment of the Open Government Directive, "OMB Watch Assesses Obama Administration's Progress on Open Government Recommendations," March 18, 2011, at http://www.foreffectivegov.org/node/11558. The Sunlight Foundation noted that many agencies met the requirements of the directive, but did not execute particular initiatives they had planned to accomplish. See The Sunlight Foundation, "Obama's Open Government Directive, Two Years On," December 7, 2011, at http://sunlightfoundation.com/blog/2011/12/07/obamas-open-government-directive-two-years-on/. *The Michigan Journal of Environmental and Administrative Law* also published an online blog post noting the mixed results of the directive and encouraged the President to continue make transparency a priority. See Eric Merron, *Michigan Journal of Environmental and Administrative Law*, "Obama's Open Government Initiative: A Progress Report," February 24, 2013, at http://students.law.umich.edu/mjeal/2013/02/obama%E2%80%99s-open-government-initiative-progress-report/.

[16] Cass R. Sunstein, *Informing Consumers through Smart Disclosure*, Office of Management and Budget, Washington, DC, September 8, 2011, at http://www.whitehouse.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf.

[17] Pursuant to the memorandum, machine readable means the data are "stored in a format enabling the information to be process and analyzed by computer," for example, formats that could be "readily imported into spreadsheet and database applications." Ibid., p. 5.

[18] Pursuant to the memorandum, standardization requires that information "be available in standardized vocabularies and formats ... that allow for meaningful comparisons and other analyses across datasets." (Ibid.)

[19] Pursuant to the memorandum, market adaptation and innovation would require agencies to "periodically consult with user communities ... to review and adapt smart disclosure regimes so that the information conveyed remains accurate and relevant." Ibid. p. 6.

[20] Pursuant to the memorandum, interoperable means that the data are more valuable if they "can be linked to other sources of data" through "common identifiers ... using consistent vocabulary."(Ibid.)

[21] Ibid, pp. 5-6.

[22] Ibid., p. 2.

[23] National Science and Technology Council, "Smart Disclosure and Consumer Decision Making: Report of the Task Force on Smart Disclosure," May 2013, at http://www.whitehouse.gov/sites/default/files/microsites/ostp/report_of_the_task_force_on_smart_disclosure.pdf.

code-a-thons and workshops that can assist in the development and demonstration of new ways to use existing datasets.[24]

The Creation of *Recovery.gov*

Another transparency-related oversight mechanism was the establishment of *Recovery.gov* in compliance with the American Recovery and Reinvestment Act of 2009 (ARRA; P.L. 111-5).[25] The website was intended to be a repository for information related to implementation and oversight of ARRA funding. The website currently includes overview information about the legislation, accountability reports and actions, frequently asked questions, and data on the distribution of funds and major recipients.

Recovery.gov was built by the Recovery Accountability and Transparency Board (RATB), a committee of inspectors general from around the federal government. The public-facing website arguably allowed "taxpayers to be in a better position to hold their government accountable."[26] While the website initially contained inaccurate information, the RATB enforced policies to remedy these errors.[27] Additionally, the federal government used the website to make public the names of those funding recipients who failed to appropriately file spending and job creation data. It is unclear, however, whether the public release of these recipients' names prompted greater compliance with federal law,[28] or whether the website increased accountability of participating agency and funding recipients.

Congress and the President have engaged in several additional initiatives that use technology to create public-facing databases that seek to use "crowdsourcing" to assist in federal oversight. Among the examples are *USASpending.gov*;[29] *Data.gov*;[30] and *Performance.gov*.[31]

---

[24] Ibid., pp. 22-25.

[25] CRS Report R40572, *General Oversight Provisions in the American Recovery and Reinvestment Act of 2009 (ARRA): Requirements and Related Issues* by Clinton T. Brass.

[26] Michael F. Wood and Alice M Siempelkamp, "Transparency in Government," *The Journal of Public Inquiry*, Fall/Winter 2010/2011, p. 2.

[27] U.S. Government Accountability Office, *Government Transparency: Efforts to Improve Information on Federal Spending*, GAO-12-913T, July 18, 2012, pp. 8-9, at http://gao.gov/assets/600/592592.pdf.

[28] See, for example, Michael Wood, *Recovery Blog*, Recovery Board, Shaming the Scofflaws, Washington, DC, March 28, 2012, http://blog.recovery.gov/2012/03/28/shaming-the-scofflaws/.

[29] *USASpending.gov* was established as a component of the Federal Funding and Accountability and Transparency Act of 2006 (P.L. 109-282). It provides information about federal contract and grant awards. For more on USASpending.gov, see CRS Report R42769, *Federal Grants-in-Aid Administration: A Primer*, by Natalie Keegan.

[30] *Data.gov* is an Obama Administration initiative that encourages agencies to proactively release federal datasets to the public. For more on Data.gov and transparency, see CRS Report R42817, *Government Transparency and Secrecy: An Examination of Meaning and Its Use in the Executive Branch*, by Wendy Ginsberg et al.

[31] *Performance.gov* was established as a component of the GPRA Modernization Act of 2010 (GPRAMA; P.L. 111-35). The website provides information about executive agency goals, measures, and programs. for more information on GPRAMA, see CRS Report R42379, *Changes to the Government Performance and Results Act (GPRA): Overview of the New Framework of Products and Processes*, by Clinton T. Brass.

II. Opportunities and Challenges for Inspectors General —Balancing Information Access With Privacy and Security

Increasing use of technology and the Internet, which has accompanied greater access to federal government records and operations, is often in tension with the protection of information from inappropriate release.[32]

As noted earlier, transparency and access can help promote an informed citizenry. Yet America's lawmakers have enacted into law certain categories of information and records that can or must be protected from public release. For example, FOIA protects information that if released could harm national security, invade someone's personal privacy, or hinder an ongoing criminal investigation.[33] Members of the federal government's oversight workforce often have to balance these tensions between access and protection.

Advances in Technology and Oversight by Inspectors General

Since 1978, Congress has authorized federal inspectors general to serve as permanent, independent, and nonpartisan units that combat waste, fraud, and abuse in the federal government (5 U.S.C. Appendix).[34] These 72 offices are using technology in a variety of ways to assist congressional oversight and make the government more effective and efficient. Three principal purposes or missions guide the offices of inspector general (OIGs):

- conduct and supervise audits and investigations relating to the programs and operations of the applicable agency;
- provide leadership and coordination and recommend policies for activities designed to (1) promote economy, efficiency, and effectiveness in the administration of such programs and operations; and (2) prevent and detect fraud and abuse in such programs and operations; and

[32] Although transparency and information protection are often discussed as being in tension, it has been argued that government openness can lead to better national security. See Thomas S. Blanton, "National Security and Open Government in the United States: Beyond the Balancing Test," in Suzanne Piotrowski, *Transparency and Secrecy: A Reader Linking Literature and Contemporary Debate*, (Lanham, MD: Lexington Books, 2010), p. 26.

[33] CRS Report R41933, *The Freedom of Information Act (FOIA): Background and Policy Options for the 113th Congress*, by Wendy Ginsberg.

[34] In addition to statutory inspectors general, other temporary and permanent inspectors general or watchdog-type organizations exist across the federal government. Some of these offices include the Government Accountability Office (GAO), which describes itself as "an independent, nonpartisan agency that works for Congress ... and investigates how the federal government spends taxpayer dollars." Additionally, a variety of federal agencies have federal ombudsmen who may assist employees internally with workforce concerns or assist the public with operational or other concerns. For more information on federal ombudsmen, see CRS Report RL34606, *Federal Complaint-Handling, Ombudsman, and Advocacy Offices*, by Wendy Ginsberg and Frederick M. Kaiser.

- provide a means for keeping the head of the applicable agency and Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations, as well as the necessity for and progress of corrective action.[35]

Such offices now exist in all Cabinet departments, many federal agencies, as well as many boards, commissions, government corporations, and foundations.

The overwhelming majority of OIGs are governed by the Inspector General Act of 1978, as amended (hereinafter referred to as the IG Act),[36] which has been substantially modified twice as well as subject to agency-specific OIG amendments.[37] The IG Act structured appointments and removals, powers and authorities, and responsibilities and duties.[38]

An OIG, depending upon its associated agency's mission, can perform oversight of internal operations or external outputs. For example, in 2009, the inspector general at the Department of Health and Human Services (the federal department charged with administering Medicare, Medicaid, and other federal healthcare programs) reportedly devoted 85% of the office's resources to reducing or preventing fraud involving healthcare program providers.[39] In contrast, that same year the Department of Homeland Security OIG (which oversees an entity with jurisdiction over a variety of agencies, including the U.S. Citizenship and Immigration Service and U.S. Customs and Border Protection) reportedly allocated 75% of the office's resources to oversight and investigations of internal operations, even though roughly 50% of the Department's resources were spent on grants and outside contracts.[40]

The vast differences in agency missions, and, therefore, OIG oversight of the agencies' missions and priorities, may lead to disparate adoption of the use of technology within the OIG community. According to a September 2011 survey conducted by the Council on Inspectors General for Integrity and Efficiency's (CIGIE's) New Media Working Group, only 26 of more than 70 OIGs reported using any form of "new media."[41] One recent publication found that social media can assist OIGs in gathering information for investigations[42] and can help keep OIGs informed about news stories, agency actions, the findings of

---

[35] 5 U.S.C. Appendix, § 2.

[36] 5 U.S.C. Appendix.

[37] The Inspector General Act Amendments of 1988 created a new set of IGs in "designated federal entities" (DFEs), which are usually found among smaller federal agencies, and added to the reporting obligations of all IGs and agency heads, among other things.[37] The Inspector General Reform Act of 2008 established a new Council of the Inspectors General for Integrity and Efficiency (CIGIE); amended reporting obligations, salary and bonus provisions, and removal requirements; and added certain budget protections for offices of inspector general.

[38] P.L. 95-452.

[39] Project on Government Oversight, *Inspectors General: Accountability is a Balancing Act*, Washington, DC, March 20, 2009, p. 23, at http://www.pogo.org/our-work/reports/2009/go-igi-20090320.html.

[40] Ibid., p. 24.

[41] Department of Homeland Security Office of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency's New Media Working Group, *Recommended Practices for Office of Inspectors General Use of New Media*, Washington, DC, September 2011, pp. 3-4, at http://www.ignet.gov/randp/cigienewmediarpt1111.pdf. The report defined "new media" as encompassing "all forms of electronic, digitalized, and interactive media, including tools that allow interactive communication with an external audience and those used solely internally." (Ibid. p. 6). Among the tools included within the working group's definition of new media were SharePoint, Wiki, audio or video podcasts, blogs, Facebook, LinkedIn, RSS Feed, Twitter, and YouTube. (Ibid., pp. 6-7).

[42] Nancy Eyl, "What Social Media Has to Offer Offices of Inspectors General," *Journal of Public Inquiry*, Fall/Winter 2012/2013, p. 21. Use of social media as an investigation tool can "establish motives, prove and disprove alibis ... provide leads" and help establish a subject's social circle. (Ibid.).

"citizen reporters," and priorities of their congressional overseers.[43] Moreover, new media can help OIGs comply with the Open Government Initiative to disseminate their own information, reports, and findings.[44]

In addition to new media technologies, OIGs may benefit from the use of IT to create additional efficiencies. For example, OIGs can use online databases and information to assist their audits and investigations. If OIGs are charged with finding agency waste, fraud, and abuse in all realms, then training and awareness of online databases, online scams, and use of social media may be necessary.

As was discussed at a series of meetings on the potential applications and complications of data analytics for oversight and law enforcement, most federal information technology (IT) systems are often designed to execute a specific program or mission, such as automate the distribution of a particular federal benefit. The IT system may not be designed to assist in determining the enforcement of eligibility requirements for the benefit program or to identify other program vulnerabilities.[45] By not incorporating the future needs of oversight officials in the design of new IT systems, some modernization efforts may limit the ability of IGs and others to use data to uncover waste, fraud, and abuse. In addition, overseers may attempt to use available data in ways that were not "originally intended, which can create challenges."[46]

OIGs may choose not to embrace all technologies. CIGIE's new media working group, for example, recommends that each OIG measure whether the benefits of a particular technology are worth its accompanying costs "based on IT resources and mission."[47]

The Challenges of Leveraging Technology

As OIGs and other oversight entities begin or continue to adopt evolving technologies, the protection of sensitive information and the creation of policies and procedures for appropriate use of IT will be of continuing concern.[48] Technology and new media can prompt complexities in information security,[49] privacy,[50] legal oversight,[51] and records collection.[52]

---

[43] Ibid. See also CRS Report R43018, *Social Networking and Constituent Communications: Members' Use of Twitter and Facebook During a Two-Month Period in the 112th Congress*, by Matthew E. Glassman, Jacob R. Straus, and Colleen J. Shogan, which analyzes congressional use of Twitter by Members of Congress. Using social media like Twitter, could allow OIGs to communicate their work to Members as well as for OIGs to better understand the priorities of their congressional overseers. See also, U.S. Government Accountability Office, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, June 2011, at http://www.gao.gov/assets/330/320244.pdf.

[44] Nancy Eyl, "What Social Media Has to Offer Offices of Inspectors General," *Journal of Public Inquiry*, p. 22. OIGs, for example, could educate the public "about waste, fraud, and abuse," "increase appropriate hotline use," and "help OIGs control the message about the work they do." (Ibid.)

[45] U.S. Government Accountability Office, *Highlights of a Forum: Data Analytics For Oversight and Law Enforcement*, GAO-13-680SP, July 2013, p. 4, at http://www.gao.gov/assets/660/655871.pdf.

[46] Ibid.

[47] Department of Homeland Security Office of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency's New Media Working Group, *Recommended Practices for Office of Inspectors General Use of New Media*, Washington, DC, September 2011, p. 18, at http://www.ignet.gov/randp/cigienewmediarpt1111.pdf.

[48] U.S. Government Accountability Office, *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, June 2011, at http://www.gao.gov/assets/330/320244.pdf.

[49] Information security requirements are authorized in the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. §§ 3541-3549). For an overview of FISMA, see CRS Report R42114, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, by Eric A. Fischer.

[50] The primary authority addressing the protection of personal privacy is the Privacy Act of 1974, amended (5 U.S.C. § 552a).

Continued use of large databases and new media may require investments in training, equipment, personnel, and other resources. Additionally, existing statutes, regulations, or policies may need to be revisited to determine whether they encumber IGs, the public, and other entities from effectively using online tools and data to assist oversight. For example, in a July 2013 document highlighting the findings of an earlier forum, GAO noted that "participants from the IG community" voiced concerns over a component of the Privacy Act (5 U.S.C. § 552a), as amended, that requires certain notification procedures in cases when automated data systems are shared between federal agencies or between a federal agency and a non-federal agency.[53] Specifically, the Computer Matching and Privacy Protection Act of 1988 (P.L. 100-503; 5 U.S.C § 552a), as amended, requires agencies to draft a written agreement about the use, purpose, and intended protections of any qualifying electronic system of records before it can be shared. Such sharing of datasets may assist overseers in proactively discovering fraudulent or incorrect applications for federal assistance or contracts—thereby, increasing program integrity.

For the purposes of the Privacy Act, OIGs are considered a separate agency from the agency or department they are authorized to audit and investigate. The Privacy Act, therefore, appears to require OIGs and any applicable agencies to draft agreements for sharing of electronic systems of records. According to members of the OIG community, these agreements can take years to complete.[54] Participants at the forum noted that the act may "threaten the principle of independence," which is codified in the Inspector General Act (5 U.S.C. Appendix). This component of the Privacy Act has been identified as a potential difficulty for the IG community since at least 1998, when the chairperson of the President's Council on Integrity and Efficiency (the precursor of CIGIE) testified before the House Committee on Government Reform and Oversight in favor of legislation that would permit certain federal agencies to match benefit applications to electronic data owned by the Internal Revenue Service.[55]

III. Transparency Initiatives Can Strengthen Accountability, But Do Not Substitute for Other Oversight Mechanisms

Online databases and new media can allow OIGs and the public to take part in the Administration's stated commitment of being more transparent and participatory. Making information available to the public and

(...continued)

[51] Legal oversight relates to the legal requirements and policies associated with the use of particular new media. General Services Administration (GSA) leads a coalition of federal agencies that created "federal-compatible terms of service (TOS)" for use of social media tools that are offered for use from particular private vendors. See HowTo.gov, "Federal-Compatible Terms of Service Agreements," at http://www.howto.gov/social-media/terms-of-service-agreements. OIGs and other federal agencies can use these TOS documents as templates and use their in-house legal oversight to amend the service agreement to better fit the individual needs of their agency.

[52] Federal records collection, retention, and maintenance are authorized in the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, and 33). For more information on how technology is affecting records collection and retention, see CRS Report R43165, *Retaining and Preserving Federal Records in a Digital Environment: Background and Issues for Congress*, by Wendy Ginsberg.

[53] GAO, Data Analytics, GAO-13-680SP.

[54] GAO, Data Analytics, GAO-13-680SP, p. 11. Other participants at the forum noted that the law may prohibit a sharing of the database itself, but did not prohibit agencies from sharing hardcopies of the same information.

[55] U.S. Congress, House Committee on Government Reform and Oversight, Subcommittee on Government Management, Information, and Technology, Hearing on H.R. 4243, H.R. 2347; and H.R. 2063, 105th Congress, 2nd session, March 2, 1998, H.Hrg. 105-143 (Washington: GPO, 1998), pp. 103-104.

to OIGs is, arguably, not an end in itself. Although data and information can contribute to a more informed citizenry and a more efficient government, the constitutionally-established structure of the U.S. government authorizes certain elected and appointed federal officials—not the public and not OIGs—to determine and execute federal policy. OIGs,[56] GAO, and other oversight mechanisms are empowered to publish their findings, research, and recommendations—but not to enforce the adoption of recommended policies. Instead, information access, if operationalized effectively, may aid stakeholders and the public in holding the federal government more accountable for its actions or inactions and prompt debates on how to make the government operate more efficiently and effectively.

Making vast amounts of data available to the public is not the same as oversight. For data and information to become helpful in federal oversight, they, arguably, must be appropriately used, clearly stated, and the results must be presented fairly. In some cases, data and analytics may not be the optimal oversight tools. Conducting personal interviews, working with whistleblowers, and site visits may remain the most effective courses of action in these cases.

Technology can assist in government oversight. It can provide new information and allow overseers to use data in innovative ways. Technology and use of new media can assist in investigations and facilitate public input on agency actions.[57] Providing interested stakeholders access to information can allow them to track where federal dollars are spent, can provide context on the methodology used to rate the most effective child safety seat, or can provide data on the spread of the flu virus. This access may help uncover fraud, improve safety, or even save lives. Technology, however, must be thoughtfully employed and sensitive data and information must remain protected.

Access to information alone, however, is not the equivalent of oversight. Oversight also involves the analysis of agency actions to evaluate economy, efficiency, and effectiveness. Moreover, public interest in oversight is not inherently uniform across issues or consistent over time. As a result, although transparency initiatives may facilitate citizen engagement in highly visible issues, it is less clear whether such initiatives encourage comparable participation in more routine oversight.

Access to information and federal datasets may enable scholars to access and analyze information and create new tools to show how government operates. To make "crowdsourcing" technologies relevant to federal oversight, however, agencies need to ensure that datasets released to the public or made available to OIGs are authoritative. Agencies may need to clarify any limitations of the data—for example, are some populations underrepresented in a dataset, or are there particular data points that may skew the data toward more extreme averages—so users are not inadvertently misled when analyzing the data.

As agencies release hundreds or thousands of datasets or vast amounts of records, users may need specialized knowledge to identify appropriate information to meet their needs. Counterintuitively, the release of data and records can decrease executive branch transparency, and, perhaps, hinder oversight. For example, users may have to sift through thousands of datasets to determine which ones include the information they seek. It may be difficult for a researcher to pinpoint the records he or she needs in a collection of similarly titled datasets. Other data may be made available in a format with which a researcher is unfamiliar.

---

[56] Pursuant to 5 U.S.C. Appendix § 3(c), "no Inspector General shall be considered to be an employee who determines policies to be pursued by the United States in the nationwide administration of Federal laws."

[57] Beth Simone Noveck, *Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens More Powerful* (Washington, DC: Brookings Institution Press, 2010).

Oversight can be performed using a variety of tools, techniques, and institutions. The release of new datasets and the use of new media can create new opportunities for oversight, can assist investigations, and can allow interested members of the public to share in working toward a more effective and efficient government. Technology, however, is not without costs. Monetary costs would include purchasing software and equipment, hiring employees who can use the technology, and training employees to keep up with evolving technologies. Non-monetary costs may include a greater risk of an information security breach, unintentional release of sensitive information, or increased challenges in meeting the requirements of particular federal laws—such as records management laws.[58]

Despite these costs and potential risks, CIGIE's New Media Working Group encourages agencies to thoughtfully and carefully embrace IT and new media. As the working group asserts, simply blocking the use of new media "does not eliminate information security threats."[59] Moreover, if crimes, ethical violations, and inefficiencies occur online, investigators and auditors will need to build their own capacity in use of IT to perform their oversight functions. Planning the implementation and use policies of IT and new media prior to their dissemination can prevent unwanted or improper releases of individuals' private information and make clear to employees the appropriate applications of the technologies. Evolving technologies may also prompt the need for Congress to reexamine existing records management and records protection statutes to ensure that they protect sensitive information appropriately and that they permit access to information that can assist in all forms of federal oversight.

Concluding Remarks

Congressional oversight is a vital component of an effective and efficient federal government. Woodrow Wilson, former president and political scientist, wrote in his 1885 research on the legislative branch

> Unless Congress have and use every means of acquainting itself with the acts and dispositions of the administrative agency of the government, the country must be helpless to learn how it is being served; and unless Congress both scrutinize these things and sift them by every form of discussion, the country must remain in embarrassing, crippling ignorance of the very affairs which it is most important it should understand and direct.

Mr. Chairman, this concludes my opening statement. Thank you again for the opportunity to testify, and I look forward to the Subcommittee's questions.

---

[58] CRS Report R43165, *Retaining and Preserving Federal Records in a Digital Environment: Background and Issues for Congress*, by Wendy Ginsberg.

[59] Department of Homeland Security Office of Inspector General on behalf of the Council of the Inspectors General on Integrity and Efficiency's New Media Working Group, *Recommended Practices for Office of Inspectors General Use of New Media*, p. 17.

Post-Hearing Questions for the Record
Submitted to Ms. Peggy Gustafson
From Senator Jon Tester

U.S. Senate Homeland Security and Governmental Affairs Committee, Subcommittee of the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing, "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce"

November 19, 2013

1. It's my understanding that the IG community has advocated for a statutory exemption to the Freedom of Information Act to ensure IG reports concerning agency vulnerabilities are protected. At the same time, CIGIE has advocated for an exemption to the burdens of the Computer Matching and Privacy Protection Act, and the Paperwork Reduction Act. How would such legislative actions enhance oversight?

   Response:

   Computer Matching
   The Computer Matching and Privacy Protection Act requires a protracted review and approval process before computer matching can be performed to identify improper or fraudulent disaster or other assistance payments. This approval process involves concurrence by program officials within the agency subject of the review, presenting significant independence concerns for the Office of Inspector General. The timely use of computer matching to identify those who improperly received Federal assistance, and subsequently removing them from the program after verification, improves program efficiency and enables the government to focus resources on eligible applicants. Moreover, timely computer matching can under optimum conditions prevent improper payments from occurring in the first instance and, even following payments, usually leads to enhanced recovery of improper payments. The Committee has recommended that the IG community be exempt from the provisions of the Computer Matching and Privacy Protection Act to facilitate review and identification of fraud.

   Paperwork Reduction Act
   The Paperwork Reduction Act (PRA) requires a lengthy and burdensome approval process for the collection of information by a Federal agency. The CIGIE has recommended that the PRA be amended to exempt the Federal IG offices from its requirements. IG Community has advocated for a change to the Paperwork Reduction Act in order to facilitate the independent reviews of IGs at least since 2000. In July 2000, the Honorable Gaston L. Gianni, Jr., who was then-Vice Chair, President's Council on Integrity and Efficiency, testified before the then-U.S. Senate's Committee on Government Affairs. IG Gianni testified that many IGs believe that being subject to the review process requirements of the PRA conflicts with their statutory mission to be independent and nonpartisan. He asserted that these requirements affect IG's ability to carry out audits and evaluations required by

members of Congress, through law or by requests, in a timely and effective manner. CIGIE continues to share the perspective of its predecessor organization-the PCIE.
While agency heads may generally supervise IGs, they are not to "prevent or prohibit the IG from initiating, carrying out, or completing any audit or investigation." Yet the PRA requires that information collections, such as OIG surveys, be subject to approval from a "senior official" of the agency and then from OMB. We recognize OMB's wealth of knowledge in the formulation and conduct of surveys. Indeed, our community may wish to informally seek its advice in the areas of survey formats, techniques, and methodologies. However, application of the PRA to OIGs has both process and substance implications.

Congress increasingly requires IGs, through law or by formal request, to conduct specific audits of agency programs in a very short time. Part of the audit process may involve gathering information or other data from surveys of agency contractors, grantees, those entities subject to agency regulation, or the public. Subjecting such surveys to the review and approval process could impact our ability to provide an accurate and professional produce under the tight deadlines required by Congress.

The substantive issue is whether Congress intended that either departmental officials or OMB have authority over OIG information collection efforts that are key to the performance of a successful audit. We note that GAO is exempted from PRA [44 USC 3502(1)(A)] and believe the statutory independence, mission, and dual reporting responsibility of IGs warrants similar relief for our Community.

5 USC § 552(b)(3) Exemption to Protect Sensitive Information Security Data
Since the Supreme Court's 2011 decision in *Milner v. Department of the Navy*, 131 S. Ct. 1259 (2011) , OIGs across the federal government have raised serious concerns that information related to federal agencies' information security may be unprotected from disclosure under the Freedom of Information Act (FOIA). Prior to Milner, a number of federal agencies, including OIGs, used the "high 2" form of FOIA's Exemption 2 to protect this sensitive information, including audit workpapers and agency records related to agency information security vulnerabilities. After Milner, this exemption is no longer available. Although other FOIA exemptions apply to classified information and documents compiled for law enforcement purposes, no exemption currently covers the extremely large area of documents that analyze, audit, and discuss in detail the information security vulnerabilities of the federal government.

CIGIE is proposing a narrow exemption covering information that "could reasonably be expected to lead to or result in unauthorized access, use, disclosure, disruption, modification, or destruction of an agency's information system or the information that system controls, processes, stores, or transmits." This language tracks with existing Federal Information Security Management Act language found in 44 USC § 354(a)(2)(A), and it is suggested that this intention be included in any legislative history that may be developed.

2. It's my understanding that CIGIE created a "reducing over-classification workgroup" to assist the IG community in sharing information and exchanging best practices. Has this workgroup made any progress in identifying and reducing over-classification? Have any other steps been taken to reduce over-classification across the OIG community?

Response:

On January 22, 2013, the CIGIE published "A Standard User's Guide for Inspectors General Conducting Evaluations Under Public Law 111-258, the *Reducing Over-Classification Act*. At the request of CIGIE's Inspection and Evaluation Committee and with the approval of the CIGIE Executive Council, the Department of Defense OIG led an effort to develop a common framework for conducting evaluations under Public Law 111-258, the *Reducing OverClassification Act*. A working group was established, consisting of the following OIGs: Intelligence Community, National Security Agency, National Reconnaissance Office, Defense Intelligence Agency, National Geospatial-Intelligence Agency, Environmental Protection Agency, Nuclear Regulatory Commission, and the Departments of State, Homeland Security, Justice, Energy, the Treasury, Transportation, Health and Human Services, and Agriculture. In consultation with representatives from the Information Security Oversight Office, this collaborative effort led to issuing this evaluation guide for OIG use when conducting evaluations.

This evaluation guide provides detailed guidance for OIGs to use in evaluating their agencies' processes and follows the tenets outlined in Executive Order 13526, "Classified National Security Information," and its implementing directive, 32 Code of Federal Regulations, Part 2001, and "Classified National Security Information." It is meant to serve as a guide, and not to be all encompassing, in order to allow for the unique requirements of each agency while maintaining a standard framework.

CIGIE's mission is twofold:

(A) address integrity, economy, and effectiveness issues that transcend individual Government agencies; and
(B) increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General.

CIGIE anticipates that its members will utilize this standardized evaluative approach to conduct reviews relative to the relevant statutes and regulations pertaining to over-classification. I understand several OIGs already have performed such evaluations, and these reports are available on the respective OIG's public website.

3. What can Congress do to encourage and enable the IG community to put more emphasis on preventing government waste and abuse before it starts?

Response:

The Inspector General Act of 1978, as amended, includes prevention and detection of fraud and abuse agency programs and operations among the OIGs' statutory purposes. To that end, many OIGs have developed risk and analytical models to guide their work, which includes leveraging technology when feasible. CIGIE ,and its committees, also serve as a hub to pursue initiatives to address challenges that transcend individual Government agencies.

For example, CIGIE has published summary reports of Inspectors General compliance with the *Improper Payments Elimination and Recovery Act of 2010* and other related legislation and Executive Orders. Pursuing efficient, electronic means to identify and prevent improper payments is a priority for the Inspector General community.

The Recovery Accountability and Transparency Board's (RATB) oversight of Federal spending pursuant to the *American Recovery and Reinvestment Act of 2009* has been acknowledged as a model for such oversight. CIGIE is fully supportive of the RATB model, and Inspectors General across government have benefited from the analytical capability of the RATB's Recovery Operations Center (ROC). Should a congressional debate ensue relative to broadening the role of the RATB (and the data analysis capability of the ROC) to include all government spending data, the CIGIE anticipates being supportive of such a legislative proposal. An independent entity that is authorized to compile and analyze spending data across government will supplement the oversight efforts of individual Offices of Inspector General and serve as a continued data analysis resource for CIGIE members.

4. What kind of training and support do new Inspectors General receive to ensure they are successful?

Response:

IGs are appointed, either by the President with advice and consent of the Senate, by the President, or by the head of a designated federal entity, without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations. Inspectors General have ready access to Inspector General colleagues through CIGIE for mentor opportunities. Inspectors General also can identify leadership or other training opportunities through CIGIE's Training Institute, the Office of Personnel Management, or other training/educational facilities.

To assist in accomplishing the mission of the CIGIE, there are seven standing committees. These committees address the audit, human resource, information technology, inspection and evaluation, integrity, investigation, and legislative needs of the community. Through the efforts of these committees, a wealth of information is made available to Inspectors General. Additionally, these committees often are charged with reviewing matters that broadly impact the Inspector General community. Their analysis and findings are made available to Inspectors General, which serve as an efficient means to address collective concerns that otherwise would be confronted individually by IGs.

For those Inspectors General being selected from within the community, they have had the opportunity to attend various training programs provided through our CIGIE Training Institute. The CIGIE Training Institute includes three academies providing a host of training programs to the 14,000 plus Federal OIG employees. The CIGIE Training Institute's courses are attended by OIG employees across the Federal government, whereby future leaders are exposed to the specialized challenges facing the IG profession.

5. Are there best practices—for example, a mentoring program where successful, seasoned IGs mentor new IGs—that would enable recently appointed Inspectors General to do their jobs more effectively? How can Congress help?

   Response:

   The CIGIE Chair, in conjunction with other seasoned IGs, routinely hosts mentoring meetings on various topics. As discussed in my response to question #4, IGs have ready access to Inspector General colleagues through CIGIE for mentor opportunities along with leadership training through the CIGIE Training Institute.

   The ability of CIGIE's Training Institute to deliver specialized training programs to the Inspector General community is dependent on available resources. The Institute is currently making training widely available and synchronized with the professional needs of its member organizations by creating a variety of courses. In the future, the Training Institute plans to shift from instructor-led to more web-based and blended learning courses. CIGIE's Training Institute goal is to create an automated gateway to responsive, high-quality, cost effective, state-of-the-art, specialized training that can satisfy the IG community's needs today and in the future.

6. How commonly do IGs train agency staff in detection and prevention of waste, fraud and abuse? Can and should they do more of this?

   Response:

   Training agency staff in detection and prevention of waste, fraud and abuse is an ongoing responsibility for OIGs. Increasing employee awareness on where and how to report fraud, waste, and abuse is a regular and recurring practice for most OIGs, to include information on whistleblower protections. Many OIGs routinely conduct specific training programs to highlight indicators of fraud, waste, or abuse based upon their experience derived from reviews and investigations. There are no aggregate statistics available relative to training conducted by OIGs for agency employees, but we believe these training programs are an effective use of the limited, available OIG resources.

7. It's my understanding that IGs conduct annual peer reviews of each other. How effective are these assessments? What other quality standards are in place?

   Response:

   External peer reviews are recognized as an effective way to ensure and improve quality within the oversight community. They allow for professionals of similar size and composition to conduct a rigorous review of an OIG's policies and work products. CIGIE coordinates a peer review program for audit and investigation functions across the IG Community, and its relevant committees provide guidance and expertise to those OIGs conducting peer reviews, as needed.

In accordance with *Government Auditing Standards* and section 6(e) of the Inspector General Act of 1978, as amended, these external peer reviews are conducted every three years, and the results are published on the respective OIG's website and discussed in an appendix to the OIG's *Semi-Annual Report to Congress*, to include information pertaining to outstanding recommendations. CIGIE periodically reviews its program guides for both audit and investigations to ensure they are current, relevant and appropriately laid out to adequately assess OIG operations in these professional areas.

CIGIE's Inspection and Evaluation Committee has long recognized the value of external peer reviews. Recently, the Inspection and Evaluation Committee developed a framework for conducting pilot external peer reviews based on CIGIE's Inspection and Evaluation quality standards, and initiated a pilot peer review program.

CIGIE maintains a list of quality standards on its website, which include:

Government Auditing Standards
Quality Standards for Digital Forensics
Quality Standards for Federal Offices of Inspector General
Quality Standards for Investigations
Quality Standards for Inspection and Evaluation

Post-Hearing Questions for the Record
Submitted to Mr. Michael E. Horowitz
From Senator Jon Tester

U.S. Senate Homeland Security and Governmental Affairs Committee, Subcommittee of the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing, "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce"

November 19, 2013

1. I want to know more about how Inspectors General work in conjunction with the Department of Justice on investigations. How do these cases progress from oversight investigations to criminal investigations? Who makes those decisions?

   Response: The Department of Justice (Department) Office of the Inspector General (OIG) investigates allegations of criminal wrongdoing as well as administrative misconduct by Department employees, contractors, and grant recipients. Allegations of criminal misconduct may include bribery, fraud, civil rights violations, and violations of other federal laws.

   In Fiscal Year (FY) 2013, the OIG received a total of approximately 12,000 complaints from a variety of sources. Many of these complaints involved non-criminal allegations of misconduct, while some involved potential criminal wrongdoing. The OIG receives these complaints from various sources including whistleblowers, the public, Congressional Members and staff, and the internal affairs offices at the Department's law enforcement components (the Federal Bureau of Investigation, Drug Enforcement Administration, U.S. Marshals Service, and Bureau of Alcohol, Tobacco, Firearms, and Explosives). Pursuant to the Inspector General Act and Department regulations, the Department is required to report to the OIG any non-frivolous allegations of waste, fraud, and abuse, as well as any non-frivolous allegations of misconduct by Department employees (with the exception of misconduct by Department attorneys that relate to the exercise of their authority to investigate, litigate, or provide legal advice; such allegations are instead referred to the Department's Office of Professional Responsibility).

   The OIG Investigations Division also receives referrals from the OIG Audit Division as a result of audits that the Audit Division has conducted. For example, many investigations have been initiated by the Investigations Division following an OIG audit of a DOJ grant where the grant recipient was suspected of misusing grant funds or stealing grant money.

   As a result of these referrals and complaints, in FY 2013, the OIG Investigations Division opened 430 investigations, which includes both administrative and criminal cases, and over 70 persons were charged with criminal offenses. The decision whether to open and pursue an investigation, including any criminal or administrative investigation, is solely that of the OIG. While the OIG has investigative authority, and therefore can make

decisions with regard to investigations, it does not have prosecuting authority. Thus, in the course of handling these investigations, if the OIG believes that an investigation involves potential criminal wrongdoing, the OIG will refer the matter to an appropriate prosecuting office for its review and consideration for criminal prosecution. While occasionally our investigations uncover potential non-federal crimes, in most circumstances the cases involve potential federal offenses. In cases that involve potential federal offenses, the Investigations Division will likely refer the investigation for review to a U.S. Attorney's Office, the Criminal Division's Public Integrity Section, or the Civil Rights Division. Ultimately, it is the Department's prosecutors, and not the OIG, who make the decision about whether to initiate a federal criminal prosecution. When a case involving potential criminal misconduct is declined by Department prosecutors, the OIG is able to continue the investigation and treat the matter as a case for potential administrative discipline. If we conclude that a non-criminal matter involves administrative misconduct, we prepare a report on our investigation and its findings, and provide it to the appropriate Department component for review and handling. The decision whether to impose discipline and what discipline to impose is made by the Department component and not the OIG.

2. How do you balance case confidentiality with the performance of oversight?

Response: The OIG is committed to effective, independent, and transparent oversight of the Department through its many audits, reviews, and investigations. The OIG also recognizes its important reporting requirements and accountability to Congress. It has been my practice and it will continue to be my practice to keep Congress informed of significant problems the OIG identifies in the Department's operations. There are, of course, certain limitations that may affect the extent and timing of disclosure (such as restrictions on disclosure of grand jury, sealed, wiretap, classified, and law enforcement sensitive information, and limitations involving disclosure of ongoing criminal investigations). However, I am committed to providing congressional notifications and briefings for Members or staff about significant problems that we may uncover, subject to the limitations described above, as soon as we have sufficient information to do so responsibly. While a criminal investigation or audit can take an extended period of time, if we conclude in the course of an investigation or audit that there are serious issues of mismanagement or waste involving Department operations, we recognize the importance of informing the Department of those issues so it can promptly remediate the problems and informing Congress so it can conduct oversight on the issue. For example, the OIG decided to issue an interim audit report regarding the Department's operation of its Witness Security Program upon finding significant issues impacting national security that we believe required an immediate remedy.

3. We know that USIS, the contractor responsible for the Snowden and Aaron Alexis background investigations, has been under criminal investigation for allegedly bypassing quality reviews to maximize profits. However, because it was a criminal investigation, case confidentiality was invoked. And Congress wasn't made aware of key weaknesses in the background investigation process even though significant fiscal and security

implications were involved. How do oversight officials balance the need to not compromise an ongoing criminal investigation with the need to keep Congress and the public informed of misconduct or waste, especially when investigations can last multiple years?

Response: Please see the response to Question 2 above.

4. The IG Act requires Inspectors General to report particularly flagrant problems to Congress through agency heads within seven days. This is known as the "seven-day letter." How frequently is the seven-day letter actually used? Is the seven-day letter a useful tool for oversight?

Response: Since my arrival as Inspector General in April 2012, we have not made any reports to the Attorney General pursuant to Inspector General Act section 5(d) due to "serious or flagrant problems, abuses, or deficiencies," and I am told that my office (DOJ OIG) did not make any such reports from January 1, 2009, to the date of my arrival. While I have not had a circumstance yet during my tenure as Inspector General where a seven-day letter was issued, I believe there could be circumstances where such a report would provide a useful tool for oversight.

5. Can you speak to the role played by Inspectors General Special Agents, particularly in terms of generating investigative recovery revenue?

Response: The investigative process conducted by OIG Special Agents is critical in cases involving potential revenue recovery and includes collecting evidence, calculating damages, and pursuing all appropriate remedies. OIG Special Agents and Forensic Auditors investigate allegations of fraud, waste, abuse, and misconduct by Department employees, contractors, and grantees. The OIG Special Agents have a critical role in ensuring appropriate remedies are pursued when financial loss is identified, including the recovery process of misused taxpayer dollars.

The OIG typically initiates fraud investigations based upon proactive OIG initiatives, qui tam False Claims Act suits, audit referrals, or reporting from Department components, employees, grantees and contractors. Such matters often result in civil settlements, recoveries, fines, and restitution. From FY 2003 to FY 2013, the OIG's Investigations Division has recovered $108,683,617.37, of which $36,809,006.93 related to civil processes and $54,856,995.62 related to criminal actions. In FY 2013, investigations by the OIG resulted in monetary recoveries totaling more than $14.1 million, which includes civil and criminal penalties, judicial and non-judicial fines, forfeitures, and restitution.

6. Your office puts out a "Top Ten" report each year on the challenges faced by the Department of Justice. As this report has not yet been released, can you talk about some of the issues you've found for this year's report?

Response: As required by law, the OIG annually issues a statement on the top management and performance challenges facing the Department. The OIG provided its most recent statement to the Department on November 12, 2013, which was included in the Department's consolidated annual financial report and issued in December 2013. The OIG's statement identifies and discusses six management and performance challenges that the OIG believes represent the most pressing concerns for the Department, as follows:

Addressing the Growing Crisis in the Federal Prison System

This challenge discusses a two-fold crisis in the federal prison system. First, the costs of the federal prison system continue to escalate, consuming an ever-larger share of the Department's budget. From FY 2001 to FY 2013, the prison population in the Federal Bureau of Prisons (BOP) facilities grew from about 157,000 inmates to about 219,000 inmates. During this same period, the budget for the BOP was $4.3 billion in FY 2001, or about 20 percent of the Department's discretionary budget, but by the end of FY 2013 the BOP's budget had grown to $6.4 billion, or 25 percent of the Department's discretionary budget. In the current era of flat or declining budgets, the continued growth of the prison system budget poses a threat to the Department's other critical programs – including those designed to protect national security, enforce criminal laws, and defend civil rights. Second, federal prisons are facing a number of important safety and security issues, notably, the annual upward trend of overcrowding. Since 2006, Department officials have acknowledged the threat overcrowding poses to the safety and security of its prisons, yet the Department has not put in place a plan that can reasonably be expected to alleviate the problem.

Safeguarding National Security Consistent with Civil Rights and Liberties

This challenge discusses the issues facing the Department's efforts to protect national security while simultaneously protecting civil rights and liberties. The section also highlights the difficulties of appropriate information sharing in the area of national security and outlines the OIG's findings in reviews of the Federal Witness Security Program, the FBI's use of National Security Letters (NSL), Section 215 of the Foreign Intelligence Surveillance Act (FISA), and Section 702 of the FISA Amendments Act. It also identifies as an emerging concern the issue of appropriate storage, handling, and use of national security information after it is lawfully acquired, including whether and how that information may appropriately be used in a criminal investigation.

Protecting Taxpayer Funds from Mismanagement and Misuse

Given the current climate of budget constraints, the Department should take particular care to ensure that it is operating as efficiently and effectively as possible. The section discusses several concrete opportunities for the Department to improve its efficiency and highlights the importance of the Department remaining vigilant in

its oversight of grant funds awarded to third parties; enforcing laws against financial offenses and fraud; and recovering money owed to the Department as a result of financial judgments and spending that money wisely. For example, a review of the Department's airfares and booking fees found that the Department has not configured its travel booking system to ensure that employees on official travel select the most cost-effective airfare available, and that it can continue to reduce travel contractor fees by maximizing the use of its online booking system. Additionally, an OIG audit identified problems with the United States Marshals Service's procurement policies and practices. The section also notes the more than $35 million in questioned costs and more than $4 million in taxpayer funds that could be put to better use that the OIG identified in its FY 2013 reports, including reports performed by independent auditors pursuant to the Single Audit Act. In addition to these identified funds, the OIG has issued numerous recommendations for program improvements to the Department that have not been quantified in dollars, many of which remain open.

Enhancing Cybersecurity

This challenge describes the serious and rapidly evolving threat posed by cyber attacks, cyber espionage, and cyber crime. Among the issues discussed is the need to ensure that all Department law enforcement agents – not just those designated as cyber specialists – are properly trained in basic cyber investigatory techniques and are provided with adequate cyber tools; the need for effective coordination of cyber specialists within the Department and with the private sector; and the growing threat of intellectual property theft. This section also discusses the Department's challenges in defending its own systems and data against increasingly sophisticated cyber criminals, including insider threats.

Ensuring Effective and Efficient Law Enforcement

This challenge addresses issues facing the Department's traditional law enforcement missions to prevent crime; to protect the American people; and to administer justice at the federal, state, local, tribal, and international levels. The Department can further clarify the missions among its law enforcement components and develop more consistent policies that incorporate best practices from across the law enforcement community. This section also discusses, among other things, the challenges of integrating emerging and rapidly evolving technologies – such as drones, GPS devices, and mobile phone technologies – into law enforcement efforts even as the legal rules governing those technologies remain in flux, and of addressing the pressing problem of crime in Indian Country and the U.S. territories.

Restoring Confidence in the Integrity, Fairness, and Accountability of the Department

Recent OIG audits, reviews, and investigations underscore the need for the Department to ensure that it strengthens and maintains its reputation for integrity,

fairness, and accountability of its personnel and its operations. The section discusses, among other things, the OIG's recent report assessing the enforcement priorities of the Voting Section of the Civil Rights Division over time and whether the voting rights laws have been enforced in a non-discriminatory fashion; instances in which Department employees made inaccurate or incomplete statements to Congress or other government entities; and the Department's efforts to administer a fair and effective disciplinary system to address instances of employee misconduct. Finally, the section discusses the OIG's view that Congress should eliminate from the Inspector General Act the limitation on the OIG's jurisdiction to handle allegations of misconduct by attorneys. Whereas the OIG is the primary oversight entity with respect to most Department employees, including all of its law enforcement agents, the Office of Professional Responsibility (OPR) is authorized by statute to investigate allegations of misconduct against Department attorneys where the allegations relate to the exercise of the attorney's authority to investigate, litigate, or provide legal advice. OPR does not have the same statutory independence as the OIG, and the Attorney General appoints and can remove the head of OPR. We believe the OIG's institutional independence when conducting misconduct investigations and its strong record of transparency are vital to ensuring effective oversight and enhancing the public's confidence in the Department's operations.

The full report can be found here: *http://www.justice.gov/oig/challenges/2013.htm.*

7. What can Congress do to encourage and enable the IG community to put more emphasis on preventing government waste and abuse before it starts?

Response: The Department of Justice OIG has long believed that one of our highest priorities is to prevent and deter government waste and abuse, as is mandated by Congress in the Inspector General Act and is committed to deterring waste and abuse through its role overseeing Department employees, programs, contractors, and grant recipients.

The OIG deters and prevents waste through, in part, the program recommendations made in our reports and reviews. The OIG's audits, reviews, evaluations, inspections, and investigations and the resulting recommendations and corrective actions contribute toward a more accountable Department. These critical oversight functions identify areas of waste, fraud, abuse, and misconduct, and also serve as formidable preventative measures and deterrents. In addition, the OIG's longstanding practice of continually monitoring the Department's progress in implementing our recommendations ensures that our concerns are being addressed in an appropriate manner and demonstrates the OIG's insistence on holding the appropriate individuals accountable. The OIG has over 1200 open recommendations for which we track and seek resolution. For example, we are currently completing follow-up reports on several of our important prior reviews, including on the Department's and ATF's controls in light of our Operation Fast and Furious report, the Department's management of the terrorist watchlist, and the FBI's use of National Security Letters and Section 215 authority. We expend significant time

and resources in connection with such follow-up efforts, and we do so because we recognize the importance of making every effort to ensure that the Department promptly addresses and effectively remedies the issues that we identify in our reviews.

Also, as mentioned above, the OIG investigates allegations of criminal wrongdoing as well as administrative misconduct by Department employees, contractors, and grant recipients. Allegations of criminal misconduct may include bribery, fraud, abuse, civil rights violations, and violations of other laws. We believe that these investigations, coupled with appropriate discipline for those who engage in misconduct, deter wasteful and abusive practices by Department employees, contractors, and grantees.

In addition to its primary oversight functions, the OIG mitigates waste and abuse in a number of other ways. The OIG uses data analytics and initiatives focused on proactive investigative techniques in order to identify fraud and potential internal control issues in their early stages. The OIG conducts intelligence-based audits and reviews to target Department programs or policies that present the highest risks of waste, fraud, and abuse. The OIG has issued training modules to recipients of federal grants, in collaboration with other Offices of Inspector General; the training materials describe the grant recipient's responsibilities to retain appropriate financial records and monitor contractors, sub-recipients, and partners in an effort to reduce the improper use of federal funds and to increase the retention of adequate financial records. In addition, the OIG aims to make whistleblowers feel comfortable in disclosing to the OIG information which may expose waste, fraud, and abuse. Such whistleblowers are the "eyes and ears" for the OIG to identify fraud, waste, and abuse before it occurs. Through these mechanisms, the OIG strives to identify and recommend remedies for waste and abuse in the Department at the earliest stages possible.

To accomplish this important oversight responsibility, it is essential that we have both the proper resources available to conduct thorough reviews and full access to the documents and materials within the possession of the Department of Justice. Appropriate funding for OIG operations enables us to conduct comprehensive reviews and determine actionable recommendations. For example, the most effective reviews are conducted onsite in the physical location of the office, component, or grant recipient. In this way, the OIG reviewers can learn about and research deeply into the underlying program materials and financial records, and we can assess first-hand the processes in place to recommend improvements. In addition, for the OIG to conduct effective oversight, it must have complete and timely access to all records in the Department's custody that the OIG deems relevant to its review. This issue is discussed in more detail in Question 8 below, but timely and direct access to all pertinent materials during the course of our review would enable a clearer understanding of the situation and allow us to make more effective recommendations.

8. You mentioned in your testimony that there have been occasions when your office has had issues arise with access to certain records due to the Department's view that access was limited by other laws. For example, issues arose in your review of Operation Fast and Furious regarding your access to grand jury and wiretap information that was directly relevant to your review, and to wiretap information that was directly related to your ongoing review of the Department's use of Material Witness Warrants. You testified that in each instance, the Attorney General and the Deputy Attorney General provided your office with written permission to receive the materials because they concluded that the two reviews were of assistance to them. Though you said that the Attorney General and Deputy Attorney General made it clear that they will continue to provide your office with the necessary authorizations to enable you to obtain records in future reviews, requiring an Inspector General to obtain a memorandum from Department leadership in order to be allowed to review critical documents in the Department's possession impairs your independence and conflicts with the core principles of the Inspector General Act. Do you think that your office needs further authority to request this type of information? Is there a legislative fix that the Subcommittee put forward?

   Response: The OIG believes that in order to conduct effective and transparent oversight, an Inspector General must have prompt and full access to all records in the agency's possession that the OIG deems relevant to its review. Indeed, Section 6(a) of the Inspector General Act specifically authorizes Inspectors General "to have access to all records, reports, audits, reviews, documents, papers, recommendations or other material available to the applicable establishment which relates to programs and operations with respect to which that Inspector General has responsibilities under this Act." Inspectors General should be provided full access to the documents of an agency, as already stipulated in the Inspector General Act. Refusing or restricting an OIG's access to relevant documents may inhibit oversight or lead to unnecessary delays in the review and report process.

   Section 6(a) of the Inspector General Act provides the authority that an OIG needs in order to obtain access to all documents it deems relevant to its review. Difficulties have arisen for us when a component has taken the position that other Congressional statutes limit an IG's access to records, despite the plain language in Section 6(a) of the Inspector General Act. We do not believe that it was the intent of Congress to limit an IG's authority through these other statutes, and we would be pleased to work with the Committee and Subcommittee in order to develop an appropriate legislative proposal to address this straightforward issue.

9. In a DOJ IG report released on September 26th, your office outlined findings that DOJ had not established specific privacy guidelines for the use of Unmanned (UAS) and was rather just issuing the same guidelines used for manned aircrafts, though UAS raise a different set of concerns as they can fly closer to homes and be in the air for much longer than traditional manned aircraft. Has the Deputy Attorney General acknowledged that privacy rules applying strictly to UAS should be developed? Has the DOJ Privacy Office been tasked with this yet?

Response: In our review of the use and support of Unmanned Aircraft Systems (UAS) in the Department, we recommended that the Office of the Deputy Attorney General (ODAG) convene a working group comprised of Department components using or with an interest in using UAS to determine whether UAS capabilities are sufficiently distinct from those of manned aircraft that they require a specific Department-level policy to address privacy and legal concerns. These concerns may arise out of UAS's unique maneuverability and capability to operate for long periods of time. The Department has confirmed that in August 2013 the Office of Legal Policy was asked to convene a working group among several Department components (including the Office of Privacy and Civil Liberties) to identify and address policy and legal issues pertaining to the use of UAS for surveillance purposes. The Department also indicated that it was participating in an interagency process that is to consider UAS-related policy issues that are shared across departments and agencies. As we do with our other reviews, we intend to continue to monitor the Department's progress in implementing our recommendations.

Post-Hearing Questions for the Record
Submitted to Ms. Carolyn Lerner
From Senator Jon Tester

U.S. Senate Homeland Security and Governmental Affairs Committee, Subcommittee of the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing, "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce"

November 19, 2013

1. Do you attribute the OSC's dramatic increase in caseload to an environment in which whistleblowers are now more comfortable coming forward?

   An active, productive OSC helps to create an environment in which whistleblowers feel comfortable coming forward. Disclosures to OSC are at all-time high both because whistleblowers trust that they will be protected if they step forward and believe the information they disclose will make a difference in correcting government wrongdoing.

   In just the past two years, OSC achieved 332 favorable actions on behalf of whistleblowers and the merit system. This is an 85% increase over the previous two-year period. Favorable actions include the relief that OSC secures for employees who are the victims of retaliation, such as back pay, reinstatement, or reassignment to a non-retaliatory environment. They also include disciplinary actions taken against employees who engage in retaliation or other prohibited conduct, as well as cases where we work with agencies to implement systemic reforms to prevent problems from recurring. Despite ongoing budget and staffing challenges, we have managed to shift more staff to the investigation and prosecution of whistleblower retaliation and other prohibited personnel practice cases. We are prioritizing the issue that matters most to whistleblowers: will I be protected if I speak out? Now more than ever, the answer to that question is yes.

   Whistleblowers also want to know if their disclosures will make a difference in correcting government misconduct. A number of high profile cases demonstrate that OSC is a safe and secure channel for reporting waste, fraud, and abuse, and also that disclosures to OSC will help to curb the reported misconduct. For example, OSC worked with whistleblowers at the Port Mortuary at Dover Air Base to ensure that problems in the handling of remains of fallen service members were identified and corrected. Because of the whistleblowers, the Air Force is now better able to uphold its sacred mission on behalf of fallen service members and their families. More recently, and as this committee is aware, OSC worked with whistleblowers in the

Department of Homeland Security to disclose widespread abuse of overtime pay authorities, which costs the taxpayers tens of millions of dollars a year.

2. What are some of the biggest threats to this environment?

OSC's potential for building on recent successes and strengthening this environment is limited by severe resource and staffing challenges. The simple mathematics of historically-high case levels and a shrinking budget poses the biggest threat to OSC in maintaining an environment in which whistleblowers feel more comfortable coming forward.

To illustrate, staffing levels at OSC are at the same level as 10 years ago. But, OSC now receives double the number of prohibited personnel practice complaints as in 2002. We also took on new responsibilities for protecting the employment rights of service members under USERRA. And, congressional enactment of the Whistleblower Protection Enhancement Act of 2012 established new mandates and responsibilities for protecting whistleblowers. OSC received the highest number of filings in its history during the first month after the Act passed, and the caseload has continued at this increased pace.

We have managed to meet these demands by more efficiently handling cases without sacrificing productivity. Indeed, our cost to resolve a case dropped by 40% in the last 5 years, a decrease of over $2,640 per case, while our number of favorable actions soared to all-time highs, as discussed above.

However, we have reached capacity in our ability to keep responding to increased demands at current staffing levels. The President's Fiscal Year 2014 budget request for OSC provides a necessary increase of approximately $1.7 million, which both the House and Senate Appropriations Committees approved. While we are currently operating, like most agencies, under a continuing resolution, I am hopeful that final spending bills for 2014 will include this modest increase.

Post-Hearing Questions for the Record
Submitted to Ms. Karen Neuman
From Senator Jon Tester

U.S. Senate Homeland Security and Governmental Affairs Committee, Subcommittee of the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing, "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce"

November 19, 2013

1. When decisions are made and policies are written at DHS, does your office have a seat at the table?

Response: Generally, yes. Section 222 of the Homeland Security Act vests the Chief Privacy Officer with "primary responsibility for privacy policy" at DHS. In this capacity, my office has issued a number of policies that govern how personally identifiable information (PII) is used by components across the department, first and foremost a Department-wide Directive on Privacy Policy and Compliance, which sets out roles and responsibilities for DHS personnel who handle personal information. In addition, my Office has issued privacy policies for the operational use of social media, privacy incident handling, protecting information within the Information Sharing Environment, safeguarding sensitive PII, and what we call our "mixed-systems" policy, which extends administrative Privacy Act protections to non-U.S. Persons whose information is held in a DHS system that also includes U.S. Person information.

In addition to these department-wide policies, we also work closely with individual programs and offices from the very earliest stages of program and system design. When contemplating a new system or use of data, components work with their own Component Privacy Officer to complete and submit a Privacy Threshold Analysis (PTA) to the DHS Privacy Office. My office then evaluates the PTA to determine whether the proposal is likely to pose privacy risks and whether existing privacy compliance documentation—Privacy Impact Assessments (PIA) and Privacy Act System of Record Notices (SORNs)—cover the program, system, or activity.

In instances where there are likely to be privacy risks, the full privacy compliance process begins, which typically includes a full PIA. As I described in my testimony before this committee, PIAs are both a process and a document. The PIA process is a close collaboration between operational components, their component privacy officers, and the DHS Privacy Office. It begins at the earliest stages of program or system development and continues throughout the entire project life-cycle. Often times the PIA document must be published before the system goes live, or the program becomes operational, or the information is shared. Periodic reviews of PIAs and SORNs, as well as newly instituted Privacy Compliance Reviews, further ensure that our engagement with programs lasts beyond our initial assessment activities.

Finally, the Privacy Office is afforded a literal seat at the table of many senior-level intra-agency committees at DHS, giving us even broader insight into departmental priorities. These include participating on the Information Sharing and Safeguarding Governance Board; the DHS Records

Working Group, which includes stakeholders for sharing DHS data and negotiating MOAs with the Intelligence Community; the Counterterrorism Advisory Board; and the Common Vetting Task Force.

The Privacy Office's efforts to operationalize privacy at DHS have coincided with a growing understanding by the American public that privacy matters. DHS leadership and operational personnel value our equities and recognize that the Privacy Office is an important partner in assuring the success of the Department's missions.

2. Are you noticing an impact on your ability to recruit and retain the skilled talent you need? What are your hard-to-fill positions, and how are you filling them?

Response: We have not noticed a change in our ability to recruit and retain skilled talent. There are many talented privacy professionals who are interested in public service. We have experienced average attrition in the Privacy Office; however, most departing employees are seeking opportunities with increased responsibility in other Federal agencies, or offices within DHS that have a critical need for experienced privacy professionals. We are proud that, within the last year alone, two seasoned managers from the Privacy Office have left the Department of Homeland Security to assume senior executive privacy leadership positions at the Departments of Treasury and Defense. The Privacy Office works hard to identify appropriate replacements for these senior privacy policy and compliance positions, which involve a strong understanding of Departmental programs and operations. We have found there are competitive candidates working for other DHS components and try to leverage the existing pool of talent within the Department, as well as external sources.

Post-Hearing Questions for the Record
Submitted to Dr. Wendy Ginsberg
From Senator Jon Tester

U.S. Senate Homeland Security and Governmental Affairs Committee, Subcommittee of the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Hearing, "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce"

November 19, 2013

1. ***Oversight offices operate in a unique space as independent agencies within the existing structure of federal agencies. While we often rely upon the oversight workforce to shed light on misconduct and waste in agencies, who is ultimately responsible for policing those who do the police work?***

   Question one is complex. To narrow its scope, I focus on oversight of the inspectors general (IGs), which are an important component of the oversight workforce. In short, some of the institutional checks on IGs include peer reviews, investigations into allegations of wrongdoing, removal of an IG from office, and congressional oversight.

   Pursuant to the Inspector General Act of 1978 (IG Act), as amended (5 U.S.C. Appendix), all offices of inspectors general (OIGs) are required to comply with the Government Accountability Office's (GAO's) auditing standards.[1] GAO's standards, the Generally

[1] IGs who are appointed by the President with the advice and consent of the Senate (so-called "establishment IGs") are required to comply with GAO's standards pursuant to 5 U.S.C. Appendix §4(b)(1)(A). IGs appointed by an agency head (so-called "designated federal entity IGs"), are required to comply with GAO's standards pursuant to 5 U.S.C. Appendix §8G(g)(1), which (continued...)

Accepted Government Auditing Standards (GAGAS), require that all federal audit organizations undergo an "external peer review performed by reviewers independent of the audit organization being reviewed at least once every three years."[2] Section 5 of the IG Act requires OIGs to include the results of any peer review conducted during the half year time period covered in each of their semi-annual reports to Congress.

In addition to peer reviews, IGs are also held accountable through investigations of allegations of wrongdoing. Section 11 of the IG Act established the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE, pursuant to Section 11, maintains an Integrity Committee, which is required to "receive, review, and refer for investigation allegations of wrongdoing" made against leadership or staff of the 72 OIGs whose IGs are members of the council. Pursuant to the IG Act, the Integrity Committee would then either refer a "potentially meritorious" allegation of wrongdoing to the appropriate agency of jurisdiction over the matter. If the allegation cannot be referred to an appropriate agency outside of CIGIE, the matter is then to be referred to the chairperson of the Integrity Committee for further investigation. Once an investigation that alleges wrongdoing is completed, the Integrity Committee is required to assess and forward the report and any "recommendations of the Integrity Committee, including those on disciplinary action, within 30 days" of the investigation's completion to

- CIGIE's executive chairperson,
- the President, the agency or establishment head,
- the House Committee on Oversight and Government Reform,
- the Senate Committee on Homeland Security and Governmental Affairs, and
- any other relevant congressional committees.

If CIGIE's Integrity Committee or an agency investigation of allegations of wrongdoing against an establishment IG was found to have merit, Congress, the President, or the applicable agency head would likely determine any appropriate response.

In some cases, Congress, the President, or an agency head can address allegations of wrongdoing or inappropriate administration of an OIG by removing an IG from his or her position. Pursuant to the IG Act, establishment IGs can be removed only by the President or through the impeachment process in Congress.[3] Pursuant to the IG Act, IGs appointed

(...continued)

makes 5 U.S.C. Appendix §4(b)(1)(A) applicable to IGs in designated federal entities.

[2] U.S. Government Accountability Office, *Government Auditing Standards*, 2011 Revision, GAO-12-331G, December 2011, p. 61, at http://gao.gov/assets/590/587281.pdf. CIGIE makes publicly available a guide for conducting peer reviews, which is available at http://www.ignet.gov/pande/audit/2012%20CIGIE%20Audit%20Quality%20Control%20and%20Assuance%20Policy%20and%20Guidelines%20March2009,%20Updated%20Nov%202012.pdf. The *Guide for Conducting External Peer Reviews of the Audit Organization of Federal Offices of Inspector General* was last updated in 2012. The document does not indicate who assigns peer reviewers to particular OIGs.

[3] 5 U.S.C. App. §3. When exercising removal authority, the President must communicate the reasons to Congress in writing 30 days prior to the scheduled removal date. This advance notice allows the inspector general, Congress, and other interested parties to examine and possibly object to the planned removal (see 5 U.S.C. App. §3(b) for PAS IGs under the IG Act; 50 U.S.C. (continued...)

by their agency head can be removed only by the agency head or by the impeachment process in Congress.[4]

Additionally, Congress, through its oversight authority, can hold hearings, write letters, request information, or perform any other of a number of actions to hold IGs accountable to their missions.[5]

2. *If an IG is not meeting personal or professional conduct standards, who steps in?*

As noted above, Congress, the President, or an agency head may address allegations of wrongdoing or inappropriate administration of an OIG by removing an IG from his or her position.

Additionally, Congress has the authority to investigate allegations of misconduct through a variety of oversight approaches, including hearings, information requests, and face-to-face meetings with the IG. As noted above, if allegations of wrongdoing or misconduct are made against an IG, CIGIE's Integrity Committee must follow statutory requirements for appropriate investigation of the allegations.

Pursuant to the IG Act, the Integrity Committee's membership consists of the following individuals:

- an official from the Federal Bureau of Investigation who serves as chairperson of the committee;
- four IGs from the federal government representing both establishment and agency-head appointed OIGs;
- the special counsel of the Office of Special Counsel;
- the director of the Office of Government Ethics; and
- the chief of the Public Integrity Section of the Criminal Division of the Department of Justice, who serves as legal advisor to the committee.

In a March 2009 report, the Project on Government Oversight (POGO) expressed some concerns that the operations of the Integrity Committee are not transparent, suggesting that even members of the OIG community are not clear on the processes and procedures the committee uses to execute an investigation.[6] Moreover, POGO stated that the Integrity Committee's structure constituted an institutional "weakness." POGO wrote:

(...continued)

§3517(b)(6) for the IG in the CIA; and 50 U.S.C. §3303(c)(4)) for the IG of the Intelligence Community).

[4] 5 U.S.C. App. §8G. When exercising removal authority, an agency head must communicate the reasons to Congress in writing 30 days prior to the schedule removal or transfer date. This advance notice allows the inspector general, Congress, and other interested parties to examine and possibly object to the planned removal. (see 5 U.S.C. App. §8G for all IGs who are appointed by an agency head).

[5] CRS Report RL30240, *Congressional Oversight Manual*, by Todd Garvey et al.

[6] Project on Government Oversight, "Inspectors General: Accountability is a Balancing Act," March 20, 2009, at http://www.pogoarchives.org/m/go/ig/accountability/ig-accountability-20090320.pdf. According to POGO's website, the (continued...)

> Not all allegations received by the IC [Integrity Committee] amount to violations of law, with which the FBI is primarily concerned. Rather, the allegations are generally about inappropriate behavior or other misconduct that, which not rising to the level of a crime, are nevertheless significant when alleged against an IG. The risk is that if the head of the Committee is trained to be looking for criminality, he or she may overlook misconduct or inappropriate behavior that does not actually violate any laws.[7]

As a policy option, Congress may choose to require the Integrity Committee to make public its investigation procedures. Alternatively, Congress may choose to maintain the current system. Allegations of wrongdoing, even those found without merit, can negatively affect an IG's reputation and ability to perform his or her duties. Congress may determine that some secrecy of operations is needed for the Integrity Committee to effectively and fairly conduct its investigations.

If Congress finds that the Integrity Committee does not adequately investigate or address allegations of professional misconduct—behavior that would not qualify as illegal or criminal—Congress may choose to examine ways to amend the structure or mission of the Integrity Committee. Congress may also consider requiring GAO to conduct investigations of allegations of wrongdoing. GAO has performed such investigations in the past.[8]

3. ***It's my understanding that IGs conduct annual peer reviews of each other. How effective are these assessments? What other quality standards are in place? What has traditionally been the case?***

As noted above, pursuant to the IG Act, all OIGs must comply with the GAGAS, which requires OIGs to undergo a peer review at least once every three years. According to CIGIE's guide for conducting peer reviews, the reviews are to

> determine whether, for the period under review, the reviewed OIG audit organization's system of quality control was suitably designed and whether the audit organization is complying with its quality control system

(...continued)

organization is "a nonpartisan independent watchdog that champions good government reforms." See Project on Government Oversight, "About POGO," at http://www.pogo.org/about/.

[7] The Project on Government Oversight, "Inspectors General: Accountability is a Balancing Act," March 20, 2009, p. 11, at http://www.pogoarchives.org/m/go/ig/accountability/ig-accountability-20090320.pdf.

[8] See, for example, U.S. Government Accountability Office, *Inspectors General: Alleged Misconduct by NASA Inspector General*, GAO/OSI-95-9,February 1995, at http://www.gao.gov/assets/230/220967.pdf; and U.S. Government Accountability Office, *GPO Office of Inspector General: Alleged Mismanagement and Misconduct by Assistant Inspector General for Audits*, GAO/OSI-97-3R, April 23, 1997, at http://www.gao.gov/assets/90/86335.pdf.

> in order to provide the OIG with reasonable assurance of conforming with applicable professional standards.[9]

CIGIE's guide to peer review does not state how the peer reviewers are selected, but does provide characteristics of the external peer review team. These characteristics include:

- having knowledge of the GAGAS;
- being independent of the OIG being reviewed, its staff, and the products that will be reviewed;
- having sufficient knowledge of how to conduct a peer review; and
- being part of an independent audit organization that passed its last peer review.[10]

Although not explicitly indicated in the peer review guide, CIGIE generally assigns a federal OIG of similar size as a peer reviewer.

CRS was unable to find evidence that CIGIE has studied the peer review system to determine whether it is effective in maintaining or improving OIG operations governmentwide. One concern that Congress may have with the current peer review system is the limited number of OIGs available to conduct peer reviews. It is possible that a department OIG would conduct a peer review of another department. OIGs could then swap roles the next year. For example, the U.S. Postal Service (USPS) OIG may peer review the Department of Defense (DOD) in one year. The followings year, DOD could be assigned to peer review the USPS OIG. The current peer review structure, therefore, may be at risk for perceived or real conflicts of interest.

POGO has criticized IG peer reviews as having "limited value," because they are "basically consisting of a week-long scrutiny of the IG's work papers to ensure they provide proper back-up for each audit."[11] POGO, in its March 2009 report, noted that the National Aeronautics and Space Administration's (NASA's) OIG successfully passed two peer reviews during the same time period GAO investigated the NASA IG and "concluded that the NASA IG had failed to address the economy and efficiency of agency operations, despite the clear mandate of the IG law to do so."[12]

---

[9] U.S. Council of Inspectors General on Integrity and Efficiency, "Guide for Conducting External Peer Reviews of the Audit Organizations of Federal Officers of Inspector General," updated November 2012, at http://www.ignet.gov/pande/audit/2012%20CIGIE%20Audit%20Quality%20Control%20and%20Assuance%20Policy%20and%20Guidelines%20March2009,%20Updated%20Nov%202012.pdf. The guide defines a *system of quality control* as encompassing "the audit organization's leadership, emphasis on performing high-quality work, and the organization's policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements."

[10] Ibid., pp. 7-8.

[11] The Project on Government Oversight, "Inspectors General: Accountability is a Balancing Act," March 20, 2009, p. 43. at http://www.pogoarchives.org/m/go/ig/accountability/ig-accountability-20090320.pdf.

[12] Ibid.

4. The Administration launched an open government initiative in 2009 designed to dramatically enhance transparency. In terms of transparency, are we better off today than we were in 2009? What are some of the successes and failures of this initiative?

The answer to this question largely hinges on how one defines transparency. There is no single definition of what constitutes transparency, nor is there an agreed-upon method for measuring it.

The Open Government Directive, which the Obama Administration released in 2009, aims to employ a proactive and participatory approach to federal transparency—requiring agencies to release a variety of new datasets to the public before they are requested.[13] The initiative also requires agencies to respond to public comments and feedback submitted to their websites.

This operationalization of transparency places some responsibility for government oversight on the general public, watchdog groups, and other interested constituencies. By requiring new datasets be made available to the public, the Obama Administration provided a tool that can be used to monitor some federal agency performance.[14] This "crowdsourcing"—or use of the collective opinions of a mass, online audience—may improve the quality of data that are released to the public. On *Data.gov*, for example, users can rate federal datasets that are made available using a five-star scale.[15] Users can click a link to "Contact Dataset Owner" and send the federal administrator of the data an e-mail with thoughts or comments. The public can also "flag" the dataset for one of five reasons: copyright violation, offensive content, spam or junk, personal information, or for some other reason.[16] Individuals who contact agencies are asked to provide their e-mail addresses to receive an agency response.

Improved access to agencies and their data may be identified as increasing federal transparency. Providing access to information, however, may also have limitations. Crowdsourcing may improve data quality, for example, but only for agencies that release datasets and choose to read and respond to comments and suggestions.[17]

---

[13] Executive Office of the President, "Transparency and Open Government," 74 *Federal Register* 4685, January 26, 2009. The memorandum was released on January 21, 2009, at http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.

[14] At a December 10, 2009, Senate Budget Committee Task Force on Government Performance hearing, both the federal CIO (then-Vivek Kundra) and the federal CTO (then-Aneesh Chopra) said that watchdog groups and members of the public would enforce agency accountability. U.S. Congress, Senate Committee on the Budget, Task Force on Government Performance, *Data-Driven Performance: Using Technology to Deliver Results*, 111th Cong., 1st sess., December 10, 2009, http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=budget121009&st=1005.

[15] See, for example, *Data.gov*, "Active Duty Marital Status," at http://explore.data.gov/Population/Active-Duty-Marital-Status/r84k-m39h.

[16] Ibid.

[17] Pursuant to the Open Government Initiative, agencies are required to respond to public input electronically received via their open government websites. Agencies, however, have responded to the Open Government Initiative's directives with varying diligence.

Some watchdog groups have offered reviews of the Obama Administration's record on transparency.[18] For instance, *PolitiFact*, a project by the *Tampa Bay Times*, examines statements made by public figures and rates the accuracy of those statements. *PolitiFact* found that the Obama Administration met its goals of releasing new data and information to the public.[19] *PolitiFact* also noted that President Obama did not make all meetings with organized interests related to health care reform open to the public, nor, *PolitiFact* stated, did the President make the regulatory process appropriately transparent.[20]

[18] One private entity's examination of the Administration's Open Government Directive, for example, was OMB Watch's (now known as The Center for Effective Government), "Leaders and Laggards in Agency Open Government Webpages," February 23, 2010, at http://www.foreffectivegov.org/node/10785/. OMB Watch also wrote a similarly mixed review follow-up assessment of the Open Government Directive, "OMB Watch Assesses Obama Administration's Progress on Open Government Recommendations," March 18, 2011, at http://www.foreffectivegov.org/node/11558. The Sunlight Foundation noted that many agencies met the requirements of the directive, but did not execute particular initiatives they had planned to accomplish. See The Sunlight Foundation, "Obama's Open Government Directive, Two Years On," December 7, 2011, at http://sunlightfoundation.com/blog/2011/12/07/obamas-open-government-directive-two-years-on/. *The Michigan Journal of Environmental and Administrative Law* also published an online blog post noting the mixed results of the directive and encouraged the President to continue make transparency a priority. See Eric Merron, *Michigan Journal of Environmental and Administrative Law*, "Obama's Open Government Initiative: A Progress Report," February 24, 2013, at http://students.law.umich.edu/mjeal/2013/02/obama%E2%80%99s-open-government-initiative-progress-report/.

[19] J.B. Wogan, "Obama's transparency record: lots of data, not as much sunlight," *PolitiFact*, July 16, 2012, at http://www.politifact.com/truth-o-meter/article/2012/jul/16/obama-report-card-transparency-sunlight/.

[20] Angie Dribnic Holan, "Obama said he'd televise health reform negotiations on C-SPAN," *PolitiFact*, July 10, 2009, at http://www.politifact.com/truth-o-meter/promises/obameter/promise/517/health-care-reform-public-sessions-C-SPAN/; and J.B. Wogan, "President Called for Transparency, but agencies haven't always followed through," *PolitiFact*, July 10, 2012, at http://www.politifact.com/truth-o-meter/promises/obameter/promise/238/conduct-regulatory-agency-business-in-public/.