"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.