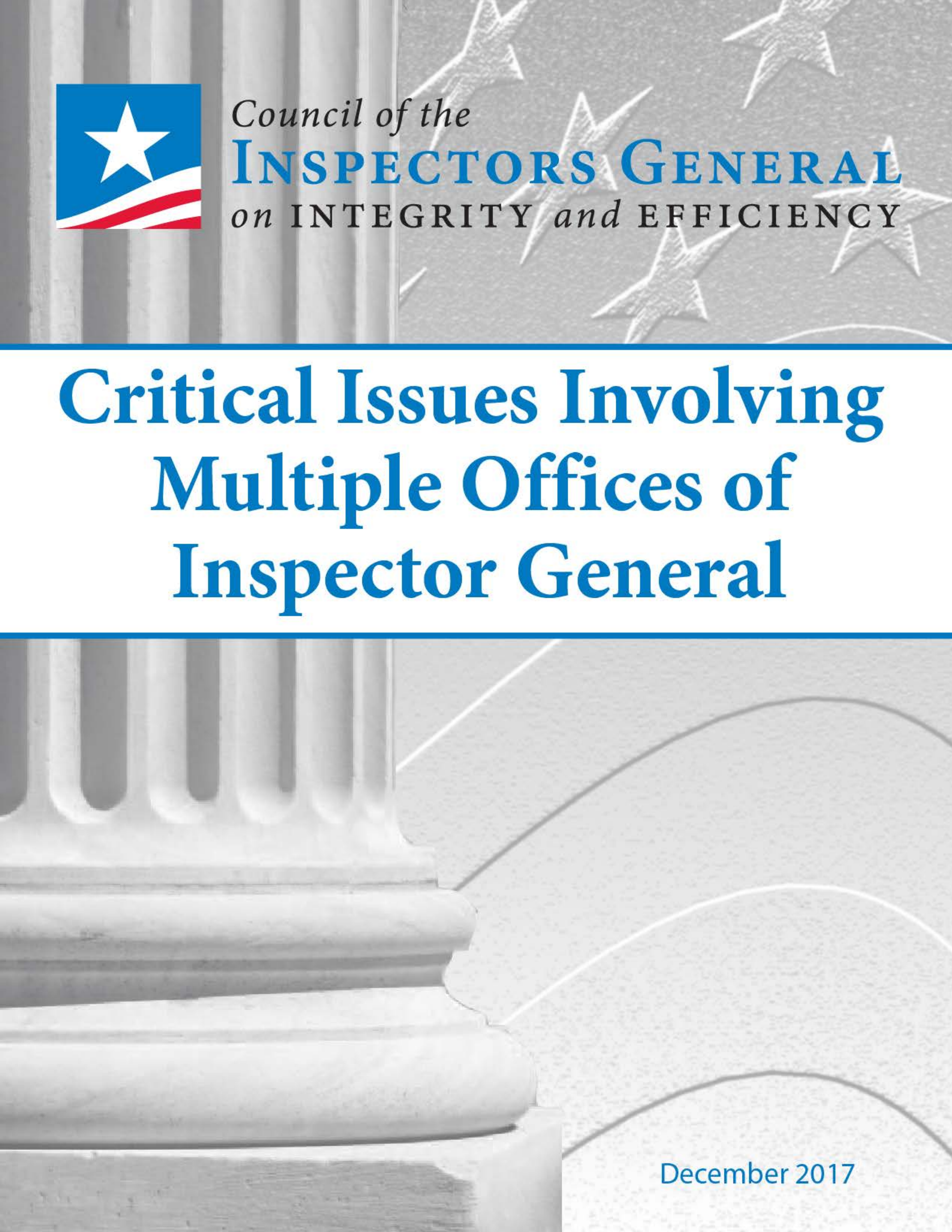

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Critical Issues Involving Multiple Offices of Inspector General

December 2017

EXECUTIVE SUMMARY

The Inspector General Empowerment Act of 2016 mandated that the Council of the Inspectors General on Integrity and Efficiency (CIGIE) conduct an analysis of critical issues that involve the jurisdiction of more than one individual federal agency. In response, we have consulted within the Inspector General community to determine six high-impact issues where coordination and collaboration would continue to be most beneficial:

- Strengthening cybersecurity
- Modernizing information technology (IT) infrastructure
- Safeguarding national security
- Ensuring integrity and efficiency in contracting and subcontracting
- Enhancing oversight of grants
- Preventing fraudulent benefit claims and improper payments

For each issue, we asked Office of Inspector General (OIG) subject matter experts to describe challenges for achieving progress on the issue, suggestions and best practices for improved coordination and collaboration, and proposals for statutory changes. CIGIE already conducts collaborative work on these issues, but discussions with the experts suggest there are opportunities to increase these efforts. Improving cross-OIG collaboration could yield a good return for federal oversight by allowing OIGs to use resources more effectively and share knowledge. In addition, it could reduce fragmentation and duplication within the government and across the oversight community.

One important new resource, Oversight.gov, is available to provide a “one-stop shop” to view work that has been issued by various individual OIGs. Although this site is primarily focused on work performed by individual offices, anyone interested in oversight can use the site to easily search a key topic area and identify individual reports covering similar issues performed by multiple OIGs. This site, which is newly launched in fiscal year 2018, will be a key resource for OIGs to promote collaboration on critical topics in the future.

CIGIE also has an important role to play. An overarching statutory change that could assist CIGIE in encouraging collaboration and coordination within the Inspector General community is to provide it with a direct appropriation. Since CIGIE was established in 2008, the method used to fund CIGIE based on assessments has not assured it the transparent, stable stream of funding it needs to meet its statutory mission. Direct funding would enable CIGIE to hire the necessary personnel to undertake important activities including encouraging deeper coordination and stronger collaboration between all OIGs.

Cross-OIG work can be more challenging than individual single-agency projects. Following the discussion of the six critical issues, this report examines the new formal remedy available for CIGIE to resolve any cross-jurisdictional disputes that emerge. It also offers best practices for OIGs to consider when conducting collaborative work. Lessons learned from past efforts could help crosscutting projects run more effectively, increase the benefits for participants, and ultimately generate more interest in future collaborative efforts. Expanding the Inspector General community’s capacity for collaborative work will improve its ability to conduct oversight across the government, particularly on these critical cross-jurisdictional issues.

TABLE OF CONTENTS

INTRODUCTION

The Inspector General Empowerment Act of 2016 requires CIGIE to conduct an analysis of critical issues that involve the jurisdiction of more than one individual federal agency to identify each issue that could be better addressed through greater coordination among, and cooperation between, individual OIGs.[1] The Act also requests that the analysis address best practices that can be employed by the OIGs to increase coordination and cooperation on each issue and any recommended statutory changes that would facilitate coordination and cooperation on critical issues.

To respond to this request, we solicited critical issues from the Inspector General community, searching for high-impact issues where coordination and collaboration would be most beneficial. We define the concept of "cross-jurisdictional" broadly, including areas where OIGs work individually on the same issues across the government as well as areas for which more than one OIG has oversight responsibility. This report addresses six critical issues:

- Strengthening cybersecurity
- Modernizing IT infrastructure
- Safeguarding national security
- Ensuring integrity and efficiency in contracting and subcontracting
- Enhancing oversight of grants
- Preventing fraudulent benefit claims and improper payments

We consider each critical issue in turn, first providing some background on current federal policy and listing recent cross-OIG work on the issue. We then describe some challenges for making progress on the issue and offer some suggestions and best practices for improving coordination and collaboration as well as proposals for statutory changes. The challenges and suggestions are based on discussions with OIG subject matter experts who conduct work in each area. After the discussion of the six critical issues, there is a brief description of CIGIE's new formal authority to resolve cross-jurisdictional disputes within the Inspector General community followed by some general best practices for cross-OIG collaboration based on interviews with participants in previous cross-OIG projects.

[1] Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, § 4(b), 130 Stat. 1595, 1600 (2016).

CRITICAL ISSUE Strengthening Cybersecurity

Cybersecurity is listed as a top management and performance challenge for many OIGs, and CIGIE and its predecessors have included "Information Technology Management and Security" as one of its Shared Management and Performance Challenges in its *Progress Report to the President* for 10 years.[2] The Government Accountability Office (GAO) likewise places cybersecurity issues on its high-risk list, including "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information" on the 2017 list.[3] For the last two years, GAO also listed information security as a material weakness in its audits of the U.S. financial statements.[4]

Current Federal Policy and the Role of OIGs

The federal government's approach to cybersecurity is governed by a matrix of laws, rules, and regulations. Most recently, Executive Order 13800 promotes enhanced cybersecurity for federal networks, national infrastructure, and the nation as a whole.[5] The executive order calls on federal agencies to implement the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST).

OIGs audit and investigate their agencies' use of IT and adoption of IT security measures under the authority of the Inspector General Act of 1978, as amended (IG Act).[6] The Inspector General community also has a key role in overseeing the effective implementation of cybersecurity requirements as part of the statutory framework of the Federal Information Security Modernization Act of 2014 (FISMA).[7] FISMA requires Inspectors General to conduct or have an independent external auditor conduct annual independent evaluations to determine the effectiveness of agencies' information security program and practices. CIGIE coordinates with the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS)

[2] For example, see CIGIE, *Progress Report to the President*, Fiscal Year 2015, http://www.ignet.gov/sites/default/files/files/FY15_Progress_Report_to_the_President.pdf, p. 13.

[3] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, Report No. GAO-17-317, February 2017, http://www.gao.gov/assets/690/682765.pdf.

[4] GAO, U.S. Government's 2016 and 2015 Consolidated Financial Statements, Report No. GAO-17-283R, January 12, 2017, http://www.gao.gov/assets/690/682081.pdf, p. 5.

[5] "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," 82 Fed. Reg. 22,391 (May 11, 2017).

[6] 5 U.S.C. app. 3.

[7] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

(continued on next page)

to develop metrics for these evaluations.[8] The results of the evaluations are published as part of OMB's annual report to Congress on FISMA.[9] Several OIGs also have the responsibility to conduct joint biennial reviews of federal cybersecurity sharing activities under the Cybersecurity Information Sharing Act of 2015.[10] As a result of these efforts, there is a significant degree of coordination within the Inspector General community around cybersecurity issues.

Recent Collaborative Work on Cybersecurity

In addition to its FISMA work, CIGIE has also conducted other cross-OIG work on cybersecurity issues. Table 1 shows recent reports. Many individual OIGs also conduct IT audits or evaluations of their agencies' cybersecurity controls beyond those required under FISMA.

Table 1: Recent Cross-OIG Work Conducted on Cybersecurity

Work	Description
Web Applications Security Cross-Cutting Project – A Federal Government Assessment of Publicly Facing Web Applications, October 3, 2017.	Nine OIGs examined cybersecurity for federal web applications at their agencies, and an additional 22 OIGs participated in a survey regarding web applications. The report identified three significant deficiencies across the agencies reviewed: incomplete and inaccurate inventories of web applications, the existence of critical and high-severity security vulnerabilities, and poorly implemented web security policies and processes.
Cloud Computing Initiative, September 2014.	The report reviewed a sample of federal contracts for commercial cloud-computing services to evaluate how agencies were adopting cloud-computing technology. It found agencies needed to include more detailed specifications in cloud contracts, meet Federal Risk and Authorization Management Program (FedRAMP) requirements, and develop accurate cloud system inventories.
Management Advisory Report: A Guide for Assessing Cybersecurity within the Office of Inspector General Community, February 2014.	The report is a high-level audit guide that can be used as a baseline for cyber and IT security-related reviews conducted by the Inspector General community.

[8] For example, see *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, V 1.0, April 17, 2017, http://www.dhs.gov/sites/default/files/publications/Final%20FY%202017%20OIG%20FISMA%20Metrics%20v1.0%20dhs%20formatted-%20508%20compliant%20v2.pdf. Beginning in 2015, CIGIE led a multi-year effort to transition the metrics to a maturity model.

[9] For the FY 2016 report, see OMB, *Federal Information Security Modernization Act of 2014 Annual Report to Congress*, March 10, 2017, http://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

[10] Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114–113, § 107, 129 Stat. 2935, 2951 (2015).

Challenges for Strengthening Cybersecurity

Subject matter experts in cybersecurity described several challenges that OIGs face in their oversight role of helping agencies strengthen cybersecurity.

Sustaining a Technically Skilled Workforce

Recruiting and training a technically skilled workforce for cybersecurity is an ongoing challenge throughout the federal government.[11] Agencies are at risk of losing skilled staff to better-paying opportunities in the private sector. This is particularly a problem for OIGs seeking to recruit individuals with cybersecurity experience to conduct audits, as these staff are expected to be skilled in both auditing standards and information technology. Where IT skills are lacking, OIGs may avoid detailed technical reviews or need to rely on contractor expertise to conduct adequate oversight.

Conducting Successful Cybersecurity Oversight for Cloud and Other Contract Services

In 2011, the federal chief information officer (CIO) announced a cloud-first policy, and in 2012, OMB followed up by advocating a shared-first approach for federal IT services.[12] The transition by federal agencies from local infrastructure to shared IT services raises new oversight questions for OIGs. How do cybersecurity risks for agencies change when services are provided in the cloud? What level of security testing is appropriate? Is there a benefit to having OIGs collaborate to avoid repeated assessments of vendors? Should OIGs evaluate agencies' monitoring of vendors or assess vendor controls directly? As described in Table 1, CIGIE has already conducted a cross-OIG project focused on cloud computing contracts. It also developed draft language to include in contracts to improve oversight access. Working together on additional cloud issues could provide benefits to the entire Inspector General community.[13]

Communicating Findings Efficiently and Effectively

The practice of preparing traditional audit or evaluation reports to inform agencies of OIG findings may not be as effective in the cybersecurity area because of the time it takes to produce reports, the risk of public disclosure of sensitive IT security issues, and the difficulty of presenting highly technical findings in a non-technical style. In some cases, by the time a report

[11] For details on federal efforts, see GAO, *Cybersecurity: Federal Efforts Are Under Way That May Address Workforce Challenges*, Statement of Nick Marinos, Director, Cybersecurity and Information Management Issues before the Subcommittee on Information Technology, Committee on Oversight and Government Reform, House of Representatives, Report No. GAO-17-533T, April 4, 2017, http://www.gao.gov/assets/690/683923.pdf.

[12] Vivek Kundra, U.S. Chief Information Officer, *Federal Cloud Computing Strategy*, February 8, 2011, http://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf and OMB, *Federal Information Technology Shared Services Strategy*, May 2, 2012, http://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2012/09/Shared_Services_Strategy.pdf.

[13] *The Council of the Inspectors General on Integrity and Efficiency's Cloud Computing Initiative*, September 2014, http://www.ignet.gov/sites/default/files/files/Cloud%20Computing%20Initiative%20Report(1)(1).pdf.

is ready, the situation has already changed. An additional challenge is that IT is a highly specialized field, in which many senior agency decision-makers do not have expert technical training.

Best Practices and Suggestions for Increasing Coordination and Cooperation

Cybersecurity is an area where there is already significant cross-OIG collaboration and coordination; however, there are opportunities for improvement.

Improve Support for OIG Cybersecurity Staff

Improved information sharing across the Inspector General community could make IT reviews more effective and spread best practices. As possible within its resources, CIGIE could explore opportunities to improve training and support for OIG cybersecurity staff. This support could include holding specialized training in auditing and other OIG skills for employees with IT backgrounds as well as providing more support to existing venues for OIG cybersecurity staff to meet and coordinate. CIGIE's Information Technology Committee provides high-level guidance on IT issues, and the Federal Audit Executive Council (FAEC) hosts quarterly meetings on IT topics at the staff level. More could be done, however, to make OIG cybersecurity staff aware of these resources. An annual forum on cybersecurity issues could help staff develop connections across the Inspector General community and raise awareness of pertinent issues. CIGIE could also promote staff exchanges such as two-way details between OIGs on cybersecurity issues to spread best practices.

One gap the subject matter experts identified is the absence of a digital space for cybersecurity practitioners within the Inspector General community to share information. While individual projects have used the federal sharing site OMB MAX for document sharing and collaboration, there is no single space for OIG cybersecurity staff to share techniques and best practices. Ideally, such a space would have both a public and a secured side so that information is readily available to interested OIG staff while any sensitive information about IT security vulnerabilities is protected from improper disclosure. It could serve a joint knowledge base on cybersecurity for the Inspector General community.

Promote Annual Focus Area for Additional Cybersecurity Projects

OIGs already spend a significant amount of resources on cybersecurity work for the annual FISMA reviews; however, some OIGs go beyond this mandated work. To promote effective targeting of critical cybersecurity issues, each year a working group could select a high-priority issue and offer background information and tools such as a draft audit or evaluation plan that would help OIGs who wished to take a deeper dive into the issue. The goal would be to promote a cross-OIG look at the critical issue. One area for which cybersecurity experts expressed a great interest in additional crosscutting work was cloud computing.

Explore Alternative Reporting Formats

Finally, given interest and the availability of resources in the Inspector General community, CIGIE could create a working group to examine modernizing the way OIGs report cybersecurity findings. The working group could solicit best practices from the Inspector General community and explore alternative formats such as shorter briefing sheets, quick response notices, electronic dashboards, or other designs that improve communication while maintaining standards and the appropriate level of independence from management.

Proposals for Statutory Changes

In the area of cybersecurity, CIGIE is proposing new legislation to protect information related to agencies' information security vulnerabilities from disclosure under the Freedom of Information Act (FOIA).[14] Although FOIA exemptions apply to classified information and documents compiled for law enforcement purposes, no single exemption covers the varied area of documents that analyze, audit, and discuss in detail the information security vulnerabilities of the federal government. Many agencies and OIGs formerly used FOIA Exemption 2, which covers records that are "related solely to the internal personnel rules and practices of an agency" to keep this information from disclosure.[15] However, in 2011, the Supreme Court clarified that Exemption 2 only protects records relating to employee relations and human resource issues, so it can no longer be used for this purpose.[16] CIGIE is proposing legislation to add a narrow exemption for records related to information security in keeping with existing FISMA language and existing requirements under FOIA to take reasonable steps necessary to segregate and release nonexempt information.

[14] Letter from Kathy A. Buller, Chair, CIGIE Legislation Committee to Dustin Brown, Acting Deputy Director, OMB, and Linda Springer, Acting Executive Chair, CIGIE, OMB, May 26, 2017, http://www.ignet.gov/sites/default/files/files/CIGIE%20Legislative%20Priorities%20115th.pdf.

[15] 5 U.S.C. § 552(b)(2).

[16] *Milner v. Dep't of the Navy*, 562 U.S. 562, 563 (2011).

CRITICAL ISSUE Modernizing Information Technology Infrastructure

Related to the challenge of strengthening cybersecurity is the need to modernize the federal government's IT infrastructure. An effective IT infrastructure is critical to support successful operations. It is also a substantive ongoing expense for federal agencies. Agencies are estimated to have spent $94 billion on IT in FY 2017, and this amount does not include amounts spent by small and independent agencies, national security systems, or classified spending.[17] In 2015, GAO added "Improving the Management of IT Acquisitions and Operations" to its annual high-risk list.[18] GAO's concerns include the problem of large failed IT projects and inadequate executive-level governance and oversight. Several OIGs have added IT management, governance, or modernization as part of their agencies' management challenges. This list includes the OIGs the Office of Personnel Management (OPM), the Social Security Administration (SSA), Amtrak, the Postal Service, and the Departments of Education, Interior, and Labor among others.[19]

Current Federal Policy and the Role of OIGs

The role of OIGs in IT modernization is to review agencies' plans and projects as part of their regular oversight work under the IG Act. Interest in improving the federal government's investment in IT systems is longstanding. The Clinger-Cohen Act of 1996 established the role of CIOs at federal agencies in law and emphasized focusing on the results of IT investments and measuring risks and benefits.[20] More recently, the Federal Information Technology Acquisition Reform Act of 2014 (FITARA) requires agencies to undertake a range of actions to increase CIO oversight over agency IT investment, improve accountability, reduce duplication, and increase cost savings.[21] FITARA mandates that agencies covered under the Act conduct self-assessments of how they will implement the Act and review those assessments annually. The law continues the federal focus on consolidating data centers to optimize and achieve cost savings that started in 2011 when the federal CIO announced a cloud-first strategy. To prevent duplication in assessing the security of cloud providers, FedRAMP provides for a standardized set of security requirements and assessment methodologies.

[17] OMB, *Budget of the U.S. Government, Fiscal Year 2018*, Analytical Perspectives, http://www.gpo.gov/fdsys/pkg/BUDGET-2018-PER/pdf/BUDGET-2018-PER.pdf, p. 191.

[18] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, pp. 58 and 180.

[19] Throughout this report, we provide examples of OIGs that included specific critical issues as part of their agency's management challenges in FY 2017. These lists are intended to be illustrative and are not exhaustive.

[20] Clinger-Cohen Act of 1996, Pub. L. No. 104–106, 110 Stat. 186 (1996).

[21] Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, § 831, 128 Stat. 3292 (2014).

Recent Collaborative Work on IT Infrastructure

As mentioned in the cybersecurity section, CIGIE published a collaborative report in 2014 evaluating how agencies were adopting commercial cloud services (see Table 2). Individual OIG reports issued in FY 2017 in this area highlight some of the challenges of modernizing IT efficiently and effectively, including developing the right strategy, keeping to schedule and budget, and balancing a desire for rapid progress with meeting security and other requirements.

Table 2: Recent Cross-OIG Work Conducted on IT Infrastructure

Work	Description
Cloud Computing Initiative, September 2014.	The report reviewed a sample of federal contracts for commercial cloud-computing services to evaluate how agencies were adopting cloud-computing technology. It found agencies needed to include more detailed specifications in cloud contracts, meet FedRAMP requirements, and develop accurate cloud system inventories.

Challenges for Modernizing IT Infrastructure

We asked OIG subject matter experts in IT to describe some of the challenges of modernizing IT infrastructure.

Sustaining a Technically Skilled Workforce

As with cybersecurity, having a technically skilled workforce to oversee IT acquisitions is important for agencies. FITARA calls for agencies to develop IT acquisition cadres to specialize in the processes of IT acquisitions and procurement. OIGs also need technically skilled staff who are capable of reviewing agencies' IT plans but who are also able to explain technical findings to a non-technical audience.

Adapting to the Cloud and Shared Services

Moving to the cloud and shared services is creating some challenges for both OIGs and agencies. When negotiating service level agreements, agencies do not always have a clear understanding of how to set requirements and ensure they have the right type and level of services to meet their needs. More guidance on how OIGs and agencies should monitor agreements would also be beneficial. For OIGs, there are questions about what information data service providers are required to share with oversight entities and how to get oversight visibility into services provided by subcontractors.

Modernizing Legacy Systems

As GAO has reported, significant work remains for agencies to modernize or replace legacy IT systems. Several systems are more than 50 years old.[22] These systems rely on outdated programming languages and can be difficult to secure, but updating them is challenging because of both a lack of funding and their size and complexity. Sometimes an incremental approach has been taken to modernization, replacing components of legacy systems rather than the whole; however, these efforts are not always viable as technology is progressing faster than agencies can incrementally modernize. Congress recently passed legislation to establish new funding mechanisms to promote IT modernization.[23]

Conducting Effective Oversight of IT Modernization Efforts

Another issue for OIGs is examining IT modernization efforts. Some subject matter experts expressed that it was not always easy to find the right criteria to evaluate whether IT modernization efforts were progressing successfully, especially from a technology perspective. More information on how to evaluate projects would be useful.

Best Practices and Suggestions for Increasing Coordination and Cooperation

Consider Cross-OIG Projects

The subject matter experts suggested that more joint OIG projects related to the cloud and shared services could be beneficial for OIGs that are interested in participating. These joint projects could help OIGs work through some of the issues related to oversight in the new environment. In addition, federal agencies frequently share cloud service providers. In these cases, conducting joint reviews might save time and effort for both OIGs and providers.

Projects focused on improving the way OIGs evaluate modernization efforts, such as developing a list of benchmarks for effective IT modernization projects or a best practices guide, would also be useful. For example, IT projects conducted using agile development methods can be challenging to audit because of the fast pace, lack of detailed estimates and documentation, and changing milestones.[24] Other suggestions for possible joint projects included examining how agencies are prioritizing IT projects, completing post-implementation reviews, implementing enterprise risk management, and training the IT workforce.

[22] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, pp. 187-8.

[23] Congress passed the Modernizing Government Technology Act of 2017 on November 16, 2017, as part of the National Defense Authorization Act for Fiscal Year 2018.

[24] Agile development methods rely on a set of principles that encourage rapid, customer-focused, iterative software development.

Improve Support for Cross-OIG Collaboration on IT Modernization

As with many of the other topics, the subject matter experts were interested in more support for cross-OIG collaboration, although they recognized there are often barriers to participating in joint projects caused by lack of time and resources. An easily accessible shared collaboration space could be helpful. Such a space could serve as a repository for lessons learned regarding IT modernization. In addition, it could help inform those interested about the latest developments and joint projects. Currently, not everyone in the Inspector General community is informed about joint work that is being undertaken.

Proposals for Statutory Changes

As federal agencies adopt cloud services, the subject matter experts suggested using legislation or regulation to provide more clarity that OIGs have access to cloud service providers' and other IT contractors' records and employees. CIGIE has proposed statutory changes to authorize OIGs to subpoena the attendance and testimony by certain witnesses, such as contractor employees or former federal employees, as necessary in the performance of the functions of the IG Act.[25]

[25] Letter from Kathy A. Buller.

CRITICAL ISSUE Safeguarding National Security

Safeguarding national security requires the cooperation of multiple agencies across the intelligence and law enforcement communities. Threats are constantly evolving and require efficient and effective information sharing mechanisms to ensure that critical information is disseminated. Agencies have made progress improving information sharing within the federal government and with state, local, and other partners. In FY 2017 GAO removed "Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland" from its high-risk list because of the progress made.[26] However, another area related to national security remains on GAO's list: "Ensuring the Effective Protection of Technologies Critical to U.S. National Security Interests."[27] Both the U.S. Department of Justice (DOJ) OIG and the Department of Defense (DOD) OIG include national security-related concerns as part of their management challenges.

Current Federal Policy and the Role of OIGs

OIGs have a responsibility under the IG Act to conduct oversight over any national security-related programs operated by their agencies. In addition, federal law includes specific oversight requirements for some agencies. For example, Section 8L(d)(1) of the IG Act requires the Chair of CIGIE to appoint a Lead Inspector General not later than 30 days after the commencement or designation of an overseas contingency operation that exceeds 60 days.[28] The USA PATRIOT Improvement and Reauthorization Act required the DOJ OIG to review the use of National Security Letters, and several OIGs were required to review their agencies' use of Section 702 of the Foreign Intelligence Surveillance Act (FISA) under the FISA Amendments Act.[29] Congressional requests have also resulted in oversight work such as the DOJ OIG's recent review of enforcement of the Foreign Agents Registration Act.[30]

Individual intelligence agencies have their own OIGs, but there is also an Inspector General of the Intelligence Community (IC IG). The IC IG conducts work across the intelligence community to find systemic problems and promote overall economies and efficiencies. The IC

[26] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, p. 4.
[27] Ibid., p. 376.
[28] 10 U.S.C. § 101(a)(13) defines a military operation as a "contingency operation" when it is (1) designated by the Secretary of Defense as an operation in which members of the armed forces are or may become involved against an enemy or opposing military force, or (2) it results in the call to or retention on active duty of members of the uniformed services.
[29] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119, 120 Stat. 192, 219 (2006) and FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).
[30] DOJ OIG, *Audit of the National Security Division's Enforcement and Administration of the Foreign Agents Registration Act,* Report No. Audit Division 16-24, September 2016, http://oig.justice.gov/reports/2016/a1624.pdf.

(continued on next page)

IG also leads the Intelligence Community Inspectors General Forum, whose mission is to promote and further collaboration, cooperation and coordination among OIGs in the intelligence community.[31] Forum members meet quarterly.

Recent Collaborative Work on National Security

Table 3 shows recent unclassified cross-OIG work conducted in the area of safeguarding national security. Most of the work done by the intelligence community is classified. Two projects evaluated the effectiveness of sharing counterterrorism information. The report on the domestic sharing of counterterrorism information was produced as a collaboration between the DOJ OIG, the DHS OIG, and the IC IG. The Boston Marathon report was conducted by the same OIGs with the addition of the Central Intelligence Agency OIG.

Table 3: Recent Cross-OIG Work Conducted on Safeguarding National Security

Work	Description
Review of Domestic Sharing of Counterterrorism Information, March 2017.	The review examines the domestic sharing of counterterrorism information.
Unclassified Summary of Information Handling and Sharing Prior to the April 15, 2013 Boston Marathon Bombings, April 10, 2014.	The report examines the extent of the information available prior to the Boston Marathon bombings and evaluates how the information was shared.

Challenges for Safeguarding National Security

The classified nature of national security work limited the discussion of challenges in this area; however, some themes emerged after consulting with experts on national security issues.

Ensuring Staff Receive and Maintain Security Clearances

At the start of FY 2017, the National Background Investigations Bureau (NBIB) was established within OPM to improve the background investigation process for security clearances. A backlog has emerged for background investigations from NBIB. As a result, some federal agencies are issuing waivers or onboarding employees for work that does not involve national security information prior to the completion of background investigations.

Having the Tools to Collaborate Successfully

Incompatible systems and tools can be a challenge for national security-related projects, particularly when it involves joint projects between agencies from the intelligence community and elsewhere in the federal government. Sometimes staff do not have the same level of clearance or use different classified systems. Project participants from some OIGs may have

[31] The forum is established by 50 U.S.C. § 3033(h)(2).

access to classified systems at their desk, while others must use a shared terminal in a separate location, slowing collaboration. During the recent collaborative review of domestic sharing of counterterrorism information, the team was ultimately able to create a shared space on an existing platform for sensitive collaboration, but technical challenges caused delays.

Best Practices and Suggestions for Increasing Coordination and Cooperation

Consider Cross-OIG Project on Background Investigations

A crosscutting project could examine whether agencies are taking a risk-based approach when they decide to issue waivers or onboard employees prior to completion of the background investigation. The project could also examine whether individuals who were brought on board without background investigations or whose reinvestigations have been delayed have criminal histories or credit issues.

Ensure Common Systems Prior to Starting a Project

Project teams, particularly on teams that mix staff from OIGs within and outside the intelligence community, should consider up front how they will share information and what systems will be used, as this can be a significant hurdle for effective collaboration.

Proposals for Statutory Changes

CIGIE currently has no formal proposals in the area of national security.

CRITICAL ISSUE

Ensuring Integrity and Efficiency in Contracting and Subcontracting

More than $470 billion was awarded in contracts across the federal government in FY 2016.[32] CIGIE lists "Procurement and Grants Management" as a Shared Management and Performance Challenge, and many individual OIGs have included contracting as a top management challenge for their agency, including the OIGs of each of the top five agencies by size of contract awards as shown in Table 4.[33] Areas of concern include conducting adequate contractor management and oversight, preventing fraud, and ensuring schedules are met and cost estimates are accurate. GAO's most recent high-risk list also includes three contracting-related items: "Department of Defense (DOD) Contract Management," "Department of Energy's (DOE's) Contract Management for the National Nuclear Security Administration and Office of Environmental Management," and "National Aeronautics and Space Administration (NASA) Acquisition Management."[34]

Table 4: Top Five Agencies for Contract Awards in FY 2016

Agency	FY 2016 Contract Funds Awarded
Department of Defense	$298 billion
Department of Energy	$27 billion
Health and Human Services	$23 billion
Veterans Affairs	$23 billion
National Aeronautics and Space Administration	$18 billion

Source: USAspending.gov

Current Federal Policy and the Role of OIGs

Contracting for most of the federal government is governed by the Federal Acquisition Regulation (FAR). As part of their oversight role, OIGs review agency contracting practices with a goal of reducing waste, fraud, and abuse. There are several remedies available to OIGs who identify contracting deficiencies. For example, they can refer contractors for suspension and debarment for a range of serious reasons such as a conviction or civil judgment for fraud. The False Claims Act allows contractors to be held civilly liable for knowingly submitting demands

[32] USAspending.gov, "Overview of Awards by FY 2008 – FY 2017," http://www.USAspending.gov/Pages/TextView.aspx?data=OverviewOfAwardsByFiscalYearTextView. This does not include contract spending by federal entities that are not required to submit data to USAspending.gov.
[33] CIGIE, *Progress Report to the President*, p. 13.
[34] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, pp. 3-4.

(continued on next page)

for payment from a government agency that contain false or fraudulent information.[35] The Program Fraud Civil Remedies Act lets agencies seek administrative civil remedies for false claims of $150,000 or less and for false statements.[36]

Under the Digital Accountability and Transparency Act of 2014 (DATA), OIGs also have a role in examining a sample of the spending data, including contract award data, that agencies submit to USAspending.gov and reporting on its quality.[37] FAEC has established a working group and put together guidance on the law.[38]

Recent Collaborative Work on Contracting and Subcontracting

Recent cross-OIG work on contracting has mostly examined ways to increase the use of tools that promote accountability, such as suspension and debarment and the Program Fraud Civil Remedies Act. Table 5 contains a list of these projects. Additionally, OIGs followed up on contract and grant spending from funds appropriated following Hurricane Sandy, and Congress established the Recovery Accountability and Transparency Board from to conduct and coordinate oversight for spending under the American Recovery and Reinvestment Act of 2009.[39] Contracting is also a focus of individual OIG efforts. A common theme of recent individual OIG reports is the need to improve administration and oversight to ensure that the appropriate policies and procedures are followed at each stage of the contracting process.

Table 5: Recent Cross-OIG Work Conducted on Contracting and Subcontracting

Work	Description
Disaster Relief Appropriations Act, 2013: Financial Status, Observations, and Concerns, September 12, 2016.	The report examines agency monitoring of spending on appropriations for Hurricane Sandy and other disasters. The spending covered contracts and grants.
Recovery Accountability and Transparency Board	The board conducted oversight over spending under the American Recovery and Reinvestment Act from 2009 to 2015.
Program Fraud Civil Remedies Act Practitioner's Guide, November 19, 2013.	The guide describes how agencies can use the Program Fraud Civil Remedies Act to pursue false claims.
Looking Inside the Accountability Toolbox: An Update from the CIGIE Suspension and Debarment Working Group, November 2013.	The document provides an update of the use of suspension and debarment across the Inspector General community following the release of a previous report on suspension and debarment.

[35] 31 U.S.C. § 3729. A related criminal version also exists at 18 U.S.C. § 1001.
[36] 31 U.S.C. §§ 3801-3812.
[37] Digital Accountability and Transparency Act of 2014, Pub. L. No. 113-101, 128 Stat. 1146 (2014).
[38] FAEC DATA Act Working Group, *Inspectors General Guide to Compliance Under the DATA Act*, Report No. Treasury OIG: OIG-CA-17-012, February 27, 2017, http://www.treasury.gov/about/organizational-structure/ig/Audit%20Reports%20and%20Testimonies/OIG-CA-17-012.pdf.
[39] American Recovery and Reinvestment Act of 2009, §§ 1521-1530, Pub. L. No. 111-5, 123 Stat. 115, 289 (2009).

Challenges for Ensuring Integrity and Efficiency in Contracting and Subcontracting

In discussions with OIG subject matter experts in contracting, some key challenges were identified.

Ensuring Adequate Contracting Oversight

Contracting within large agencies is often decentralized, with responsibilities for contract administration and oversight shared between separate contracting offices. Staff levels are not always adequate to match workloads. Improved oversight, staffing, and training for contracting officers (COs) and contracting officer representatives (CORs) would be beneficial to ensure they understand and can carry out their roles and responsibilities.[40] In some cases, OIGs find issues that simple due diligence could have uncovered before the contract started. Training on how to search for these red flags could help prevent later problems. COs also do not always review past performance assessments before awarding contracts, and contractor performance assessments can be inconsistent, with different staff giving different ratings for similar performance.

Developing Contract Cost Auditing Capabilities

The Defense Contract Audit Agency (DCAA) conducts contract audits for the Department of Defense and some other federal agencies. It plays an important role throughout the contracting process by directly auditing contractors. In the last few years, a backlog emerged for incurred cost audits, which examine whether a contractor’s costs are allowable and are a critical step prior to closing out certain types of contracts. The 2016 National Defense Authorization Act required DCAA to stop conducting any audits for non-defense agencies until the backlog was reduced to less than 18 months.[41] This resulted in a suspension of non-defense audit work from January 7, 2016, until October 1, 2016. Agencies, who previously relied on DCAA for this work, were forced to seek other ways to conduct this work. The suspension highlighted the fact that many OIGs that rely on DCAA do not have the capability to conduct audits of cost-type contracts.

Ensuring Oversight by Prime Contractors

Prime contractors are supposed to manage the subcontractors on their contracts and ensure that the appropriate federal regulations are enforced. COs and CORs are expected to make sure that prime contractors carry out their responsibilities such as ensuring that subcontracts comply with contracting policies and regulations and that subcontractor charges are sufficiently documented.

[40] In 2010, the Department of Commerce OIG, on behalf of the Recovery Accountability and Transparency Board, examined the issue of contract and grant staffing by surveying 29 OIGs to determine whether agencies awarding contracts and grants under the American Recovery and Reinvestment Act had the proper staffing, qualifications, and training. At the time, the report found that workload from the Act had put a strain on a significant portion of agencies. In addition, compliance with federal requirements varies by position for the contracting workforce, while there were no government-wide requirements for the grants workforce. Recovery and Transparency Board, *Review of Contracts and Grants Workforce Staffing and Qualifications in Agencies Overseeing Recovery Act Funds*, March 2010, http://www.oig.doc.gov/OIGPublications/arrasurvey.pdf.

[41] National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 893, 129 Stat. 726, 952 (2015).

However, sometimes COs and CORs are not ensuring that this occurs. Contracting officials do not always understand the extent of their responsibilities for administration and oversight or have sufficient resources to carry them out. Making sure that prime contractors are meeting these requirements is important because the federal government has no direct contractual relationship with the subcontractors even though subcontract costs contribute to the overall cost of the contract.

Increasing Support for Prosecuting Highly Technical Cases

Assistant U.S. Attorneys, who must balance a range of cases, can be less willing to take on prosecutions in highly specialized areas such as contracting, particularly if cases rely on statutes that are not commonly litigated. More resources to support prosecutions of these types of cases would be useful for deterrence. The DOJ already has a program to detail attorneys with specialized experience temporarily from the rest of the government as Special Assistant United States Attorneys. The program could be expanded to provide additional support in this area.

Best Practices and Suggestions for Increasing Coordination and Cooperation

Consider Cross-OIG Projects

A cross-OIG project focused on evaluating the procurement workforce might provide useful insights into what staff, training, qualifications, and abilities are needed. The project could explore the quantity and value of awards that contracting officers in different agencies are overseeing. The project could also examine the consistency of contractor performance ratings across the federal government.

Improve Support for Cross-OIG Contracting Collaboration

FAEC has a standing committee on contract audit issues, which has previously held forums on contracting issues. As with cybersecurity, continued support for regular forums on contracting issues and best practices and an easily accessible shared workspace would help those who review contracting across the Inspector General community.

Some OIGs are already using analytics to identify anomalies in contract spending and proactively identify issues. CIGIE’s Information Technology Committee sponsors a Data Analytics Working Group to encourage more OIGs to adopt data analytics. In addition, the DATA Act and other federal efforts are increasing the amount of accessible financial and payment data in a uniform format on contracts as well as grants and loans. However, barriers still exist to sharing some forms of contracting data. Interested OIGs could hold discussions about the best way to collaborate on sharing contracting data for analytics.

Consider Suggesting an Expansion of the Special Assistant U.S. Attorney Program

If there were sufficient interest and resources within the Inspector General community, CIGIE could evaluate suggesting to DOJ that the current program for Special Assistant U.S. Attorneys be expanded to offer a more permanent program. OIGs could provide the program with attorneys having an in-depth knowledge of agency-specific statutes, programs, and cultures.

Proposals for Statutory Changes

CIGIE's recent crosscutting project on increasing the use of the Program Fraud Civil Remedies Act was spurred by a 2012 GAO report that found the Act was underutilized.[42] CIGIE is also proposing several statutory changes to encourage use of the Act including increasing the dollar amount of claims subject to the Act, changing wording to bring the Act in line with the False Claims Act, and revising the definition of hearing officials for agencies that do not have access to Administrative Law Judges. More details about these changes are available from the description of CIGIE's legislative priorities for the 115th Congress.[43]

[42] GAO, *Program Fraud Civil Remedies Act: Observations on Implementation*, Report No. GAO-12-275R, January 27, 2012, http://www.gao.gov/assets/590/587978.pdf.

[43] See Letter from Kathy A. Buller.

CRITICAL ISSUE

Enhancing Oversight of Grants

The federal government awards grants for a wide range of purposes from large transportation projects to small research studies. The government awards more in grants than it does for contracts. More than $660 billion was awarded in FY 2016. Table 6 shows the top five agencies for grant awards. Of those agencies, the OIGs for the Departments of Education and Health and Human Services (HHS) and the U.S. Agency for International Development (USAID) include grants in their top management challenges. Several other OIGs also include grants as a management challenge including the OIGs for the Departments of State, Justice, Commerce, and Homeland Security as well as for NASA and the National Science Foundation.

Table 6: Top Five Agencies for Grant Awards in FY 2016

Agency	FY 2016 Grants Funds Awarded
Health and Human Services	$455 billion
Department of Transportation	$58 billion
Department of Education	$44 billion
Department of Agriculture	$34 billion
U.S. Agency for International Development	$11 billion

Source: USAspending.gov

Current Federal Policy and the Role of OIGs

OIGs conduct oversight of grants awarded by their agencies as they do for other federal programs. Grants are governed both by Part 200 of Title 2 of the Code of Federal Regulations, known as the Uniform Guidance, and supplemental guidance from individual agencies. The Uniform Guidance was issued in 2013 as a result of a three-year collaborative effort by the cross-agency Council on Financial Assistance Reform (COFAR) to streamline and consolidate federal guidance for grants.[44] CIGIE's Grant Reform Working Group contributed by regularly coordinating with OMB and providing comments and suggestions from the Inspector General community. Despite the Uniform Guidance, however, the grant process generally has more variation across the government than the process for contracts.

[44] "Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards; Final Rule," 78 Fed. Reg. 78,590 (December 26, 2013).

Recent Collaborative Work on Oversight of Grants

Table 7 shows recent cross-OIG work related to grants. Much of the work relates to both contracting and grants. CIGIE, however, is currently conducting a project on grants and other services for Alaskan Natives or American Indian populations. There are also two ongoing interagency working groups on grant fraud. One under the leadership of the DOJ OIG and the Financial Fraud Enforcement Task Force focuses on grant fraud enforcement issues; the other focuses on investigations for waste, fraud, and abuse in the Small Business Innovation Research (SBIR) grant program. In addition, individual OIGs issued grant-related work in FY 2017. One consistent theme of that work is the need for more monitoring and oversight of grantees.

Table 7: Recent Cross-OIG Work Conducted on Grants

Work	Description
Review of OIG Oversight of Alaskan Native/American Indian Funding and Programs, Ongoing.	The CIGIE Alaskan Native/American Indian Committee includes OIGs whose agencies fund grants or deliver services to Alaskan Natives or American Indian populations. The committee's current project is surveying previous OIG work regarding grants or services to these populations.
Grant Fraud Working Group	The purpose of the working group is to foster collaboration among DOJ attorneys, the OIG community, and others regarding the most effective ways to identify, investigate, and prosecute grant fraud.
SBIR investigations working group, see workshop.	The working group's goal is to prevent and detect fraud, waste, and abuse in the SBIR/Small Business Technology Transfer (STTR) program.
Recovery Accountability and Transparency Board	The board conducted oversight over spending under the American Recovery and Reinvestment Act from 2009 to 2015.
Disaster Relief Appropriations Act, 2013: Financial Status, Observations, and Concerns, September 12, 2016.	The report examines agency monitoring of spending on appropriations for Hurricane Sandy and other disasters. The spending covered contracts and grants.
Grant Reform Working Group	The CIGIE working group coordinated with OMB to provide comments and suggestions to ensure accountability safeguards were preserved in the Uniform Guidance for grants.
Program Fraud Civil Remedies Act Practitioner's Guide, November 19, 2013.	The guide describes how agencies can use the Program Fraud Civil Remedies Act to pursue false claims.
Looking Inside the Accountability Toolbox: An Update from the CIGIE Suspension and Debarment Working Group, November 2013.	The document provides an update of the use of suspension and debarment across the Inspector General community following the release of a previous report on suspension and debarment.

Challenges for Enhancing Oversight of Grants

In discussions with grant subject matter experts, several concerns about grant oversight emerged.

Ensuring Adequate Support for Grant Applicants and Officers

The subject matter experts noted that the root of many problems with grant awards was a lack of resources and training on both sides of the grant process. Some grant officers may be responsible for too many awards to review grant applications and monitor grant performance effectively. Moreover, pressure to award funds quickly and make sure funding is spent can lead to less focus on conducting due diligence. Grant recipients, particularly smaller ones, may not be aware of their obligations under the grant. Providing more information about the requirements of the award upfront during the initial award conference and ensuring that recipients certify on a regular basis that they are aware of these requirements could be helpful.

Monitoring Grant Performance

Grant officers face problems monitoring grant performance including ensuring compliance with grant requirements. Lack of transparency in spending is a significant challenge. Each award has an approved budget, and grantees must file financial reports detailing spending in broad budget categories; however, the government does not always know how each dollar is being spent unless there is an audit or an investigation.

Non-federal entities that spend more than $750,000 annually in federal awards must have an independent auditor conduct an audit under the Single Audit Act and submit information about the audit to an online clearinghouse, but there are challenges for using this information for oversight and risk assessment.[45] OIGs do not always have the resources to provide effective oversight for the more than 30,000 single audits filed annually. Moreover, only a limited amount of summary data is provided in a format that is easily accessible for analytics. More detailed summary data would make it easier for OIGs to use their limited resources to determine the highest risk grantees.

It can be particularly difficult to monitor grants when spending passes down to a subgrantee. For example, many grants go to state agencies, which then disburse them. In some cases, funds pass through several entities before reaching the final beneficiaries. In addition, agencies are also not always measuring effectiveness to ensure grants are achieving their goals for end users.

Finally, while OIGs focus on reviewing the financial aspects of grants, investigating research grants to find instances where researchers fail to meet basic research standards is less common, although it does occur. While technically challenging, such work can help ensure that grants are achieving their objectives.

[45] Single Audit Act, Pub. L. No. 98-502, 98 Stat. 2327 (1984) (codified, as amended, at 31 U.S.C. §§ 7501-7507).

Preventing Duplication and Fragmentation

Grants are given out by many agencies across the government, and there is a risk of substantial duplication and fragmentation. For example, in 2012, GAO found that there were 209 federal programs administered by 13 agencies aimed at promoting science, technology, engineering, and math (STEM) education. Most of the programs overlapped, but fewer than half of the agencies engaged in coordination with other agencies having similar programs.[46]

There is also a risk that multiple agencies could be funding the same research. Some OIGs undertake computer matching and analytics to check whether grant projects are already being funded elsewhere. GAO has added two items involving grants to its annual list of opportunities to reduce fragmentation, overlap, and duplication: (1) selected subagencies it reviewed were not ensuring that grant applications were reviewed for potential duplication and overlap and (2) fragmentation in grants for transit resilience projects.[47]

Best Practices and Suggestions for Increasing Coordination and Cooperation

Consider Cross-OIG Projects

There are several collaborative projects that might be beneficial in the grants area for interested OIGs:

- Examine duplication and fragmentation in a particular grant topic area, as GAO did for STEM education projects,
- Explore which budget categories in grants funding produce the highest risk and costs for grants, and
- Review grant procedures at various agencies from award through closeout to evaluate for consistency and effectiveness.

Expand Data Analytics in the Grant Area

Although some OIGs already are using analytics to find problems with grants, developing more analytics capacity in the grant area would be useful as more grant data is becoming available through the DATA Act. OIGs could collaborate on the difficult work of merging available federal data sets and awardee financial data to ensure federal grant funds are used properly. Combining analytics with information sharing about grant recipients could also help avoid

[46] GAO, *Science, Technology, Engineering, and Mathematics Education: Strategic Planning Needed to Better Manage Overlapping Programs across Multiple Agencies*, Report No. GAO-12-108, January 2012, http://www.gao.gov/assets/590/587839.pdf.

[47] GAO, *2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, Report No. GAO-17-491SP, April 2017, http://www.gao.gov/assets/690/684304.pdf**,** p. 4.

duplication of funding requests and identify requestors that have previously abused grant programs.

Develop a Community of Interest around Grants

While working groups in the area of grants already exist, such as the Grant Fraud Working Group and the SBIR investigations working group, creating a broader community of interest within CIGIE around grants would be beneficial given the fragmented nature of grant spending across the government. This community could promote information sharing and connections. It could include a collaborative working space with a public face, occasional forums on grant issues, and regular meetings or informal meetups.

Proposals for Statutory Changes

Aside from changes to the Program Fraud Civil Remedies Act, which are discussed in the contracting section, CIGIE's current list of legislative priorities includes no statutory proposals related to grants.[48] However, the subject matter experts had some suggestions for regulatory changes.

Adding language to grant regulations on the presumption of loss to the United States when fraud occurs could improve OIGs' ability to pursue investigations when grant recipients intentionally misrepresent their eligibility for a grant.[49] This language would state that the entire grant is a loss if the grant awardee lied to obtain the funding. Such a change would reduce the burden on investigators and prosecutors of determining the loss that resulted from the misrepresentation. Changing the regulatory language on mandatory disclosures for grants to more closely match that in the FAR would also be helpful for OIG oversight. While the current language requires grant award recipients to disclose violations of federal criminal law involving fraud, bribery, or gratuity violations, it does not include the credible evidence standard, which strengthens the mandate by requiring disclosure when there is credible evidence of these violations. In addition, the current language does not require recipients to report violations to the appropriate OIG or mention the need to report violations under the civil False Claims Act as well as criminal violations.

Another suggestion was to further improve standardization of current grant rules and procedures. COFAR, which was working on standardizing the grants process across the government, was disbanded in June 2017.[50] Finally, rules that would require grant recipients to file detailed grant spending information in a data-friendly format would make conducting oversight more efficient.

[48] Letter from Kathy A. Buller.

[49] The Small Business Jobs Act of 2010 established a similar presumption of loss for contracts, grants, and other agreements set aside for small businesses whenever a business willfully misrepresents its size and status. Small Business Jobs Act of 2010, § 1341, Pub. L. No. 111-240, 124 Stat. 2504, 2543 (2010).

[50] OMB, M-17-26, *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, June 15, 2017, http://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-17-26.pdf.

CRITICAL ISSUE Preventing Fraudulent Benefit Claims and Improper Payments

Benefit payments make up the largest share of federal spending. Social Security, Medicare, and income security programs alone accounted for more than $2 trillion in payments, more than half of federal spending.[51] Because benefit claims are such a large portion of federal spending, they also account for a substantial share of federal improper payments, which are defined as payments that should not have been made or were made in an incorrect amount. Payments for fraudulent claims are improper payments, although improper payments do not have to result from fraud. OMB designates certain programs as high priority for improper payments. Table 8 shows the top five high-priority programs based on the amount of improper payments.[52] GAO considers the government's inability to determine the full extent to which improper payments occur and and reasonably assure that appropriate actions are taken to reduce them a material weakness.[53] Improper payments for Medicare and Medicaid are also on GAO's FY 2017 high-risk list.[54]

Table 8: Top Five Programs Based on Improper Payment Amount in FY 2016

Program	Agency	Improper Payment Amounts	Rate (Improper/Total Payments)
Medicare Fee-for-Service	HHS	$41.1 billion	11.0%
Medicaid	HHS	$36.3 billion	10.5%
Earned Income Tax Credit	Treasury	$16.8 billion	24.0%
Medicare Advantage (Part C)	HHS	$16.2 billion	10.0%
Supplemental Security Income (SSI)	SSA	$4.2 billion	7.4%

Source: PaymentAccuracy.gov

Current Federal Policy and the Role of OIGs

The Improper Payments Information Act of 2002 (IPIA) first required executive agencies to submit estimates of improper payments to Congress each year.[55] IPIA was amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and the Improper Payments

[51] "Budget Functions," http://beta.USAspending.gov. Income security programs include support for low-income individuals, federal employee retirement and disability programs, food and nutrition assistance, housing assistance, and unemployment compensation.
[52] "High-Priority Programs," http://PaymentAccuracy.gov/high-priority-programs/.
[53] GAO, U.S. Government's 2016 and 2015 Consolidated Financial Statements, p. 5.
[54] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, pp. 2-3.
[55] Improper Payments Information Act of 2002, Pub. L. No. 107-300, 116 Stat. 2350 (2002).
(continued on next page)

Elimination and Recovery Improvement Act of 2012 (IPERIA).[56] Under the amended requirements, agencies must review programs that may be susceptible to improper payments and estimate the amount involved, take action to reduce improper payments, and report on the results. OMB is required to compile a list of high-priority programs having improper payments for greater oversight. OIGs must verify if executive branch agencies are in compliance with certain provisions of law. For 2015, only nine of the 24 agencies listed in the Chief Financial Officers Act of 1990 (CFO Act) were deemed in compliance.[57]

The Fraud Reduction and Data Analytics Act of 2015 (FRDA) takes further steps to prevent fraud.[58] It requires OMB to establish guidelines using GAO's Fraud Risk Framework for agencies to identify and assess fraud risks and develop controls to prevent fraud. Agencies are required to report on their fraud risks and reduction strategies in their annual financial reports. The FRDA also calls for OMB to establish a working group to improve the sharing of fraud controls and data analytics and to develop a plan for a federal interagency library of data analytics and data sets for use by agencies and OIGs.

Recent Collaborative Work on Benefit Claims and Improper Payments

CIGIE has issued two reports on improper payments as shown in Table 9. Both examine the work OIGs conducted as part of their response to federal requirements for improper payments. There is also an ongoing CIGIE project to apply data analytics to purchase card transaction data. In addition, several OIGs have joined an initiative led by the Federal Trade Commission (FTC) OIG to acquaint OIGs that investigate benefit fraud with the FTC's Consumer Sentinel Network, a secure database of consumer complaints available to law enforcement, including OIG investigators. Finally, individual OIGs conducted work on improper payments in FY 2017 beyond the standard IPERA reviews. Some of these reports examined in more detail the reasons behind specific categories of improper payments.

[56] Improper Payments Elimination and Recovery Act of 2010, Pub. L. No. 111-204, 124 Stat. 2224 (2010) and Improper Payments Elimination and Recovery Improvement Act of 2012, Pub. L. No. 112-248, 126 Stat. 2390 (2013).
[57] "IPERA Trend Table," FY 2015, http://PaymentAccuracy.gov/ipera/. The CFO Act, as amended, establishes the position of Chief Financial Officer in 24 of the largest federal agencies (31 U.S.C. § 901).
[58] Fraud Reduction and Data Analytics Act of 2015, Pub. L. No. 114-186, 130 Stat. 546 (2016).

Table 9: Recent Cross-OIG Work Conducted on Benefit Claims and Improper Payments

Work	Description
Examination of Purchase Card Transactions, Ongoing.	The project is a collaboration of 23 OIGs who are analyzing purchase card payments to look for risky transactions.
Collaboration to promote the use of the FTC's Consumer Sentinel Network to support OIG benefit fraud investigations	The FTC OIG and FTC Bureau of Consumer Protection have collaborated with other OIGs to promote the use of the Consumer Sentinel Network in OIG investigations of benefit fraud such as schemes to redirect or fraudulently obtain government benefits. The network includes more than 13 million consumer complaints and a variety of analytical tools.
Summary of Inspector General Compliance with the Improper Payments Elimination and Recovery Act of 2010, March 2013.	The report examines whether OIGs performed IPERA reviews in a timely manner and summarizes their conclusions on whether their agencies complied with the law.
Summary of Inspector General Reports Related to Executive Order 13520 on Improper Payments, August 2012.	The report summarizes the work OIGs conducted in response to Executive Order 13520 on reducing improper payments and eliminating waste in federal programs.

Challenges for Preventing Fraudulent Benefit Claims and Improper Payments

Subject matter experts on benefits, fraud, and improper payments described challenges in two main areas.

Ensuring Consistency in OIGs' Findings under IPERA

OIGs found that most covered agencies were non-compliant with IPERA's requirements; however, recent audit work by GAO determined that OIGs' compliance determinations were inconsistent.[59] Similar findings appeared to yield assessments of compliance or noncompliance depending on the OIG. Some OIGs only verified whether agencies had met the individual IPERA requirements (such as publishing the information in an annual report) as required under current OMB guidance; others went further and considered how well agencies had met the requirement (such as by examining the quality of the published information).[60] GAO attributed the cause of this inconsistency to a lack of guidance on what evaluative procedures should be used to make compliance determinations and recommended that OMB coordinate with CIGIE to develop and issue guidance. CIGIE agreed to coordinate with OMB. The subject matter experts

[59] GAO, *Improper Payments: Additional Guidance Could Provide More Consistent Compliance Determinations and Reporting by Inspectors General*, Report No. GAO-17-484, May 2017, http://www.gao.gov/assets/690/685006.pdf.

[60] OMB, Appendix C to OMB Circular A-123, M-15-02, *Requirements for Effective Estimation and Remediation of Improper Payments*, October 20, 2014, http://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-02.pdf.

noted that decisions on what approach to take in a compliance assessment were often driven by resource concerns.

OMB's guidance suggests optional work that OIGs may conduct on improper payments. GAO found that OIGs also varied in how much of this optional work they conducted, although most conducted at least one optional evaluation. These additional evaluations were useful for uncovering problems with agencies' efforts to meet IPERA requirements. Again, decisions on undertaking additional optional reviews are also likely driven by resource concerns and priorities for oversight work.

Further Improving Ability to Obtain and Share Data

The subject matter experts expressed an interest in moving from reactive audits and investigations to find fraud and other problems to a more proactive stance using analytics that could uncover issues at the beginning. To make this transition, OIGs still need more support to obtain and share data. The Inspector General Empowerment Act of 2016 greatly improved the ability to share data for oversight purposes by providing an exemption to the Privacy Act's computer matching provisions for OIG oversight work.[61] Computerized data comparisons are exempt so long as the match is performed in connection with an audit, investigation, inspection, evaluation, or other review authorized under the IG Act. However, agencies and OIGs still must comply with other requirements in the Privacy Act, such as the limits on disclosing records without the written permission of the person to whom the records pertain except under certain exceptions. CIGIE has prepared guidance to help OIGs with the data matching requirements.[62]

In addition, for many types of benefits, agencies rely on recipients to self-report changes in status. OIGs try to look for changes that have not been reported to detect fraud or improper payments, but this data is not always available. For example, very few states report marriages. In other cases, agencies are willing to share data with other agencies' OIGs in aggregate form or with personally identified information (PII) removed, but this makes the data less useful for analytics. While tax data on income is used in some data matching cases, some subject matter experts said that access to additional fields such as address, marital status, number of dependents, and self-employment status would also be helpful.

Best Practices and Suggestions for Increasing Coordination and Cooperation

Opportunities for collaboration emerged through research and discussions with the subject matter experts.

[61] Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, § 2, 130 Stat. 1595, 1595 (2016). For Privacy Act, see 5 U.S.C. § 552a.
[62] CIGIE, *Guide to the Inspector General Empowerment Act's Computer Matching Exemption*, June 2017, http://www.ignet.gov/sites/default/files/files/CMA%20Exemption%20Overview%20Guidance%20(June%202017).pdf.

Improve Consistency in OIG Findings under IPERA

CIGIE has already stated that it will work with OMB as needed to develop additional guidance for work under IPERA.

Continue Focus on Data Sharing and Analytics

Data analytics is particularly useful in the area of benefits fraud and improper payments. CIGIE and the Inspector General community have taken several steps to increase the use of analytics. In 2013, GAO, CIGIE, and the Recovery Accountability and Transparency Board sponsored a forum to explore the opportunities and challenges of using data analytics for oversight and law enforcement.[63] Representatives from federal, state, and local government, as well as from the private sector, participated. The forum identified a list of next steps for promoting the use of analytics. One of the challenges raised was ensuring that oversight and law enforcement entities were aware of available data that can aid analytics. The three forum sponsors also led the effort to compile a directory of data sources from the Inspector General community and post it on a sharing site on OMB MAX. CIGIE's Data Analytics Working Group has reached out to OIGs to update the list for FY 2017. The list could help provide a valuable starting point for compiling the interagency library of data analytics and datasets mandated by the FRDA. As CIGIE explores training and forums on data analytics, it should consider training on the use of these tools.

The Data Analytics Working Group also hosted a one-day forum in June 2017 to share information and best practices throughout the Inspector General community.[64] Around 100 people attended in person and another 200 participated remotely. CIGIE is also working to establish a community of practice for data analytics. The Interagency Fraud and Risk Data Mining Group meets quarterly to share best practices and to discuss emerging oversight areas.[65] Additional collaborations are occurring in specific topic areas; however, more could be done to build and promote connections between OIG staff working on data analytics in particular fields such as medical provider fraud, medical claimant fraud, or other types of benefits fraud. These types of collaborative groups could help solve data problems and promote improved sharing. CIGIE could encourage these efforts by adding to its website a simple list of ongoing data sharing collaborations with a contact reference point.

Proposals for Statutory Changes

To improve data sharing related to benefits fraud, CIGIE has proposed amending the Privacy Act of 1974 to expand the definition of "routine use."[66] Under the Privacy Act, disclosure for routine use is one of the exceptions to the requirement that agencies must have written permission to

[63] GAO, CIGIE, and Recovery Accountability and Transparency Board, *Highlights of a Forum: Data Analytics for Oversight & Law Enforcement*, Report No. GAO-13-680SP, July 2013, http://www.gao.gov/assets/660/655871.pdf. GAO followed up the forum by establishing its Government Data Sharing Community of Practice, which held several meetings on data sharing and analytics until it ended in 2016. See GAO, Government Data Sharing Community of Practices, http://www.gao.gov/aac/gds_community_of_practice/overview#t=0.

[64] For details on the forum, see http://www.ignet.gov/events/2017DataAnalyticsForum.

[65] The Interagency Fraud and Risk Data Mining Group, http://www.va.gov/oig/ifrdmg/.

[66] Letter from Kathy A. Buller.

disclose someone's records to another person or agency. Another exception is for law enforcement purposes. Currently, some records used as part of OIG employee benefit fraud investigations may be controlled by another agency. While the law enforcement exemption can be used to share records for law enforcement actions, it does not apply to agencies' administrative actions. The routine use exemption is an alternative. However, the agency that owns the records can prohibit their use for administrative action by another agency by deeming fraud "not compatible with the purpose for which the information was collected." Such a prohibition could frustrate the capacity of an employing agency to take administrative action against an employee for defrauding the program. CIGIE is suggesting an amendment to the Privacy Act to clarify that preventing fraud in federal benefits programs is an inherent purpose in administering and collecting information for the programs and, therefore, a permissible routine use.

IMPROVING COORDINATION AND COLLABORATION

The six critical issues this report describes are very different, but some common themes emerge in the discussion:

- A well-trained workforce with sufficient resources is a key factor for success for both agencies and OIGs.
- Data analytics is becoming an increasingly important tool for success in many areas, spurred by programs to improve data quality and availability.
- The federal government is a highly complex, highly varied organization, but there are opportunities to reduce fragmentation and duplication in specific programs.
- In keeping with the complexity of the government, OIGs conduct a wide variety of oversight work, but greater collaboration, including the use of virtual collaboration sites, may provide opportunities for OIGs to take a more unified approach to oversight in specific areas.

These themes suggest that improving support for cross-OIG collaboration and coordination could yield returns for the Inspector General community. Improved collaboration would allow OIGs to use resources more effectively and share knowledge, particularly in areas such as data analytics. It could also reduce fragmentation and duplication within the government and across the oversight community.

One overarching statutory change that could assist CIGIE in encouraging improved collaboration and coordination within the Inspector General community is to provide it with a direct appropriation. Since CIGIE was established in 2008, it has made significant strides in building the infrastructure to carry out its role; however, the methods used to fund CIGIE have not assured it the transparent, stable stream of funding it needs to meet its statutory mission. Direct funding would enable CIGIE to hire the necessary personnel to undertake important activities including encouraging deeper coordination and stronger collaboration between all OIGs.

Collaboration can be difficult and time-consuming, and individual OIGs face different oversight priorities and resource constraints that may limit their participation in collaborative efforts. In addition, sometimes OIGs disagree about how to conduct oversight on a particular issue. The following sections describe the new framework the Inspector General Empowerment Act established to resolve these cross-jurisdictional disputes and offer some best practices learned from past cross-OIG projects for collaborating more effectively.

Resolving Cross-Jurisdictional Disputes

The Inspector General Empowerment Act gave CIGIE a new responsibility to resolve cross-jurisdictional disputes between OIGs.[67] CIGIE now has the duty to receive, review, and mediate any cross-jurisdictional disputes submitted in writing regarding an audit, investigation, inspection, evaluation, or project except for matters coordinated among Inspectors General in the intelligence community. CIGIE leadership has long taken an informal role in helping OIGs resolve cross-jurisdictional concerns. Such disputes are rare, and no OIGs have made a request for mediation under the new provision since passage of the Act in December 2016. Nevertheless, this new authority provides a useful formal process to resolve any cross-jurisdictional disputes that may occur in the future.

Good coordination is an effective remedy to avoid cross-jurisdictional disputes, but it requires careful effort. For example, GAO recently reviewed coordination between the four OIGs that conduct oversight in Afghanistan: DOD, State, USAID, and the Special Inspector General for Afghanistan Reconstruction (SIGAR).[68] GAO examined the objectives of the reports issued by these OIGs from January 2015 through September 2016 as well as special projects issued by SIGAR and did not find duplication, suggesting the success of existing coordination mechanisms. GAO nevertheless recommended that the OIGs add documentation of agreed-upon roles and responsibilities in the area of reporting requirements. GAO considers this type of documentation a leading practice for effective interagency collaboration, which other OIGs that conduct cross-jurisdictional efforts may want to employ where appropriate.

Best Practices for Collaborative Projects

To understand how OIGs could collaborate on joint projects more effectively, we interviewed former participants in crosscutting projects conducted within the Inspector General community. The interviews focused primarily on projects that led to a joint report, but the lessons learned can be applied to many different types of collaboration. Five general best practices for collaboration emerged from the discussions.

- Clearly articulate the costs and benefits of a project
- Select effective leadership for collaborative projects
- Plan in detail
- Ensure consistent expectations and standards
- Forge collaborative project teams and communities of interest

[67] Inspector General Empowerment Act of 2016, Pub. L. No. 114-317, § 3(2)(C), 130 Stat. 1595, 1596 (2016).

[68] GAO, *Documented Agreement of Certain Roles and Responsibilities Could Further Enhance Coordination in* Afghanistan, Report No. GAO-18-6, November 2017, http://www.gao.gov/assets/690/688119.pdf.

Clearly Articulate the Costs and Benefits of a Project

A successful cross-OIG project requires OIGs to contribute resources and time. Ensuring adequate support for the project from the participants is critical, and one key factor is to communicate the scope of work so OIGs can decide upfront whether they have adequate capacity to participate. Some OIGs have few resources to take on discretionary work; others may have to withdraw from the project as other priorities emerge. Presenting a detailed proposal or even a draft project plan prior to the start of a project will allow OIGs to gauge the resources needed. Choosing projects that create benefits for participants and communicating those benefits can also drive participation. For OIGs that are already planning to do work in a particular area, collaborations such as sharing a common audit or evaluation plan can create efficiencies that reduce the cost. Potential projects should also be announced with enough lead-time so that OIGs can include them in their existing planning process. In addition, individuals leading projects should recognize that a smaller group of committed, dedicated participants may collaborate more effectively than a large group that is only weakly interested in the project.

Select Effective Leadership for Collaborative Projects

Projects fare better when a committed OIG takes responsibility for shepherding them from start to finish. For projects with a varied group of participants, joint leadership by small and large OIGs may be beneficial to cover different perspectives. A strong project lead is also important. Research suggests that leadership of cross-governmental projects can be more difficult than leadership within an existing organizational structure. It requires strong interpersonal skills, flexibility, the capacity to work with others whose perspectives may be different, and the ability to build trust.[69] OIGs can help recruit leaders for joint projects by encouraging the role as a development opportunity.

Plan in Detail

Many of the group project participants who were interviewed suggested that planning was a critical factor for success. In particular, they wished that they had done more planning — not only of the steps needed to achieve the project objectives but also of all the tasks needed to produce the final product or reach the end goal. OIGs can have different reporting formats, writing styles, approval timeframes, and review practices. OIGs may not share the same software or tools for conducting analysis. Early planning and discussions around these issues can avoid unexpected problems and delays.

[69] Jane Fountain, *Implementing Cross-Agency Collaboration: A Guide for Federal Managers*, IBM Center for the Business of Government, 2013, http://businessofgovernment.org/article/implementing-cross-agency-collaboration-guide-federal-managers, pp. 19-25.

Ensure Consistent Expectations and Standards

Inconsistencies in timing or work results can arise because OIG staff may not have common expectations about the final product or goal, may run into obstacles or resource constraints, may be trying to simultaneously meet the group project requirements while doing their own projects, or may come from different backgrounds such as auditing or evaluations. Too much variation can lead to difficulties crafting a consistent final report. As part of the planning process, project teams should define the final product and set ground rules including timing and the standards to be followed. If various OIGs want to participate at different levels of work, projects can be set up with flexibility, such as by having a fixed core that everyone will join with optional add-ons.

Forge Collaborative Project Teams and Communities of Interest

Because cross-government and cross-OIG projects operate outside the normal organizational structure, it is important to build trust and a sense of mutual responsibility by developing strong working relationships between team members. Frequent meetings and the use of a virtual collaboration space can help foster a cohesive project team. Beyond project teams, building communities of interest for important issues can promote collaboration by forging connections throughout the Inspector General community at the staff level. Collaboration sites, meetings and informal meetups, and annual forums where experts across the community share their experiences can all contribute to creating a collaborative community.

CONCLUSION

Cross-OIG work is often more challenging than conducting work on a single agency, but adopting best practices from past efforts can help projects run more effectively. In addition, improving collaboration through joint projects and communities of interest benefits the Inspector General community as a whole. It fosters valuable connections between experts at different OIGs and allows OIGs to share some of the planning and other developmental costs for projects that affect more than one OIG. One example is the savings from sharing the costs of preparing and merging datasets for analytics. Joint projects also allow the community to report results consistently across multiple agencies, providing useful comparison information. We believe the newly launched website Oversight.gov will be an important factor in promoting more joint project efforts and collaboration within the OIG community. Finally, joint work allows OIGs to address cross-jurisdictional issues, including the six critical issues described in this report, more effectively. Expanding the Inspector General community's capacity for collaborative work will improve its ability to conduct oversight across the government.