Post-Hearing Questions for the Record
Submitted to Beryl Davis
From Senator Claire McCaskill

"Oversight of Small Agencies"
April 10, 2014

Legislation currently being drafted by the Subcommittee would require the Government Accountability Office (GAO) to conduct a risk analysis and make recommendations to Congress about how frequently statutorily required audits, such as audits under the Federal Information Security Management Act (FISMA) and the Improper Payments Act (IPERA), should be conducted.

Does GAO think that this is a workable request?
Would GAO propose an alternative approach?

GAO response: The Federal Information Security Management Act of 2002 (FISMA) requires, among other things, that each agency both report annually on its information security programs and obtain an annual independent evaluation to determine the effectiveness of its information security program and practices.[1] The evaluations are required to be performed by the agency's inspector general (IG) or an independent external auditor. In addition, FISMA requires the Comptroller General to periodically evaluate and report to Congress on the adequacy and effectiveness of the agencies' information security policies and practices, and implementation of provisions of the act.

GAO has recognized the nation's increasing dependency on computerized information systems and electronic data. The security of these systems and data is essential to protecting national and economic security, public health, and safety. Federal information security has been on GAO's list of high-risk areas since 1997. In 2003, GAO expanded this high-risk area to include cyber critical infrastructure protection. This includes risks to information and communication systems from insider threats by disaffected or careless employees and business partners, escalating and emerging threats from around the globe, the ease of obtaining and using hacking tools, the steady advance in the sophistication of attack technology, and the emergence of new and more destructive attacks.[2]

Threats to systems supporting critical infrastructure and government information systems are evolving and growing. The number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team more than doubled in recent years from 29,999 in fiscal year 2009, to 61,214 in fiscal year 2013. In addition, reports of cyber

---

[1]FISMA was enacted as Title III of the E-Government Act of 2002, (Pub. L. No. 107-347, 116 Stat. 2899, Dec. 17, 2002).

[2]GAO, *High-Risk Series, An Update*, GAO-13-283 (Washington, D.C.: February 2013).

incidents affecting national security, intellectual property, and individuals have been widespread, with reported incidents involving data loss or theft, economic loss, computer intrusions, and privacy breaches. To illustrate, for fiscal year 2013, 18 of 24 major federal agencies reported that information security control deficiencies were either a material weakness or significant deficiency in internal controls over financial reporting. Further, for fiscal year 2013, the IGs at 21 of 24 agencies cited information security as a major management challenge for their agencies.[3]

Because of the number and significance of threats to information security throughout the federal government, we believe the current annual FISMA requirements should remain in place. As recommended in our recent update of high-risk areas, executive branch agencies need to continue to expand their oversight of information security programs and practices, and to (1) develop and implement remedial action plans for resolving known security deficiencies of government systems, (2) fully develop and effectively implement agency-wide information security programs as required by FISMA, and (3) demonstrate measurable progress in addressing deficiencies.

We are concerned that an additional GAO assessment of risks and vulnerabilities to federal agencies' information systems to determine the frequency of audit requirements would result in a duplication of requirements already in effect. Nevertheless, an alternative approach could involve GAO summarizing the results of the FISMA reviews reported by a sample of small federal agencies to help determine the benefits of providing this information on an annual basis.

The Improper Payments Elimination and Recovery Act of 2010 (IPERA)[4] amended the Improper Payments Information Act of 2002 (IPIA)[5] and enacted some new provisions. As amended, IPIA requires executive branch agencies to review all of their programs and activities to identify those susceptible to significant improper payments.[6] For programs that are considered susceptible to significant improper payments,[7] agencies must perform an annual statistically valid estimate of the program's improper payments, publish the results of that estimate, and implement a plan to reduce improper payments in the program or activity. IPERA requires agencies to conduct recovery audits, where cost effective, for each program and activity with at least $1 million in annual program outlays. In addition, IPERA calls for federal agencies' IGs to annually determine whether their respective agencies are in compliance with key IPERA requirements and to report

---

[3]GAO, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches*, GAO-14-487T (Washington, D.C.: Apr. 2, 2014).

[4]Pub. L. No. 111-204, 124 Stat. 2224 (July 22, 2010).

[5]Pub. L. No. 107-300, 116 Stat. 2350 (Nov. 26, 2002).

[6]Under IPIA, as amended, improper payments are statutorily defined as any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. According to guidance from the Office of Management and Budget, agencies should also report as improper payments any payments for which insufficient or no documentation is found.

[7]For fiscal year 2014 and thereafter, a program's improper payments are considered "significant" if they may have exceeded either $10 million and 1.5 percent of program outlays, or $100 million.

on their determinations. Federal agencies reported improper payment estimates totaling $105.8 billion[8] in fiscal year 2013.[9]

The federal government continues to face challenges in determining the full extent of improper payments. IGs have reported deficiencies related to compliance with the criteria listed in IPERA for fiscal year 2012 at their respective federal entities, including risk-susceptible programs that did not report improper payment estimates, estimation methodologies that were not statistically valid, and risk assessments that may not accurately assess the risk of improper payments. However, a number of actions are under way across the federal government to help advance improper payment reduction goals. Completing these initiatives, as well as designing and implementing enhanced strategies to include identifying and analyzing the root causes of improper payments is key to developing effective corrective actions and implementing the controls needed to reduce and prevent improper payments. Effective monitoring and reporting will be important to help detect any emerging improper payment issues.

We believe the annual IPERA requirements are important to help identify and reduce improper payments throughout the federal government. With regard to small agencies in particular, IPERA already includes provisions that reduce its administrative burden where appropriate. If a program's risk assessment determines that the program is not susceptible to significant improper payments, no further estimation is required, and that risk assessment does not have to be performed again for 3 years, absent any major changes in the program. Further, recovery auditing efforts under IPERA are only required where the responsible agency determines that they would be cost-effective. In addition, the annual requirement for the IGs to determine and report on their agencies' compliance with IPERA's provisions is a necessary oversight mechanism to help ensure that the agencies' actions are effective. Therefore, we do not believe that an additional risk assessment by GAO to determine the frequency of audit requirements under IPERA is warranted.

One of the issues that the Subcommittee is considering is whether all inspectors general should be presidentially-appointed and Senate-confirmed (PAS). I understand that GAO conducted a survey in 2011 that looked at issues of independence and found that opinions were mixed.

Does GAO believe there are enough safeguards in place to ensure that non-PAS IGs are independent?

---

[8]The estimated $105.8 billion in improper payments excludes the Department of Defense's (DOD) Defense Finance and Accounting Service (DFAS) Commercial Pay program. In May 2013, we reported on major deficiencies in DOD's process for estimating fiscal year 2012 improper payments in the DFAS Commercial Pay program. According to its fiscal year 2013 agency financial report, DOD is reevaluating its sampling methodology for fiscal year 2014 for the DFAS Commercial Pay program based on our recommendation. Consequently, the fiscal year 2013 improper payment estimate for the DFAS Commercial Pay program may not be reliable. See GAO, *DOD Financial Management: Significant Improvements Needed in Efforts to Address Improper Payment Requirements*, GAO-13-227 (Washington, D.C.: May 13, 2013).

[9]GAO, *Financial Audit: U.S. Government's 2013 and 2012 Consolidated Financial Statements*, GAO-14-319R (Washington, D.C.: Feb. 27, 2014).

GAO response: The Inspector General Act of 1978, as amended (IG Act) created offices of inspectors general at major departments and agencies with IGs who are appointed by the President, confirmed by the Senate, and may be removed only by the President with notice to Congress stating the reasons.[10] The IGs are to prevent and detect fraud and abuse in their agencies' programs and operations; conduct audits and investigations; and recommend policies to promote economy, efficiency, and effectiveness. In 1988, the IG Act was amended to establish additional IG offices in designated federal entities (DFE) defined by the act. Generally, the DFE IGs have the same authorities and responsibilities as the presidentially appointed IGs but there is a clear distinction—they are appointed by, and may be removed by their agency heads and they are not subject to Senate confirmation.

Our fiscal year 2011 survey of the IGs did not specifically address the matter of IG independence related to appointment by an agency head versus appointment by the President.[11] However, in fiscal year 2002 we did report the results of our survey of the IG community on the effect that conversion of IGs appointed by their agency heads to appointment by the President with Senate confirmation would have on IG independence.[12] Our survey also asked how the independence of DFE IG offices would be affected by consolidating their offices with larger, presidentially appointed IG offices. While the results of our prior report may not necessarily reflect the opinions of the current IGs, the responses by the presidentially appointed IGs at that time generally indicated that conversion to presidential appointment and Senate confirmation would strengthen DFE IG independence. The DFE IGs, in general, indicated that there would be no effect on their independence.

Regarding the possible impact of consolidating DFE IG offices with presidentially appointed IG offices, the presidentially appointed IGs who responded to our 2002 survey indicated that both the DFE IGs' actual independence and appearance of independence would be strengthened. The DFE IGs generally indicated that there would be no impact. The presidentially appointed IGs also indicated that several elements affecting the DFE IGs' quality of work would be strengthened through consolidation, including the ability to issue hard-hitting reports when necessary, to audit issues of high risk, to review issues across agencies, to get attention to recommendations made by the IGs, and to plan work. In addition, the presidentially appointed IGs indicated that consolidation could strengthen the DFE IGs' (1) use of resources by increasing control over spending and budget requests, (2) availability of investigative resources, (3) ability to minimize duplication of audit efforts, and (4) ability to share methods and technology specialists and to use human capital skills efficiently. At the same time, the DFE IGs generally indicated that there would be either no effect or that these elements would be weakened through consolidation.

---

[10]Pub. L. No. 95-452, 92 Stat. 1101 (Oct. 12, 1978) *codified, as amended*, at 5 U.S.C. App.

[11]GAO, *Inspectors General: Reporting on Independence, Effectiveness, and Expertise*, GAO-11-770 (Washington, D.C.: Sept. 21, 2011).

[12]GAO, *Inspectors General: Office Consolidation and Related Issues*, GAO-02-575 (Washington, D.C.: Aug. 15, 2002).

We believe that the appointment and removal processes of the presidentially appointed IGs versus those IGs appointed by their agency heads result in a clear difference in the level of independence of the IGs. Generally, the further removed the appointment source is from the audited entity, the greater the level of independence. However, safeguards to IG independence are included in provisions of the IG Act that apply to all IGs. These protections are necessary in large part because of the unusual reporting requirements of the IGs, who are both subject to the general supervision by the heads of the agencies they audit and expected to provide independent reports of their work externally to Congress. In addition, *Government Auditing Standards* recognizes that safeguards exist for the independence of DFE IGs.[13] These safeguards are specified by provisions in the IG Act and include (1) establishment of the IGs by statute, (2) communication to Congress of the reasons for an IG's removal, (3) statutory protections that prevent the audited entity from interfering with an audit, (4) statutory requirements for the audit organization to report to a legislative body on a recurring basis, and (5) statutory access to records and documents related to agency programs.

[13]GAO, *Government Auditing Standards, 2011 Revision*, GAO-12-331G (Washington, D.C.: December 2011).