From: Douglas Hileman, CRMA, CPEA, P.E.
To: Yellow Book Comments
Subject: Comments on GAGAS Exposure Draft (April 2017)
Date: Thursday, July 06, 2017 7:30:10 PM

COMMENTS TO THE GAO

I am pleased to submit comments to the Government Accountability Office (GAO) on the 2017 Exposure Draft of Government Auditing Standards, published in April 2017. I am president of Douglas Hileman Consulting LLC (DHC), now in its tenth year. I have over 30 years of experience in auditing, including in-house compliance audits, environmental/ safety/ sustainability audits, Internal Audit (using both GAGAS standards and the Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF)), specialist support to financial assurance teams, and as a lead auditor for the conflict minerals Independent Private Sector Audits ((IPSAs), as a non-CPA auditor using GAGAS performance standards). I hold credentials as Certified Risk Management Assurance professional and Certified Professional Environmental Auditor (granted and managed by the IIA) and Fundamentals in Sustainability Accounting (granted and managed by the Sustainability Accounting Standards Board). I am active in the IIA, including on a global committee that writes guidance documents for the Internal Audit profession. I am a co-author of "Internal Audit and the Second Line of Defense" and other thought leadership and knowledge briefs in conjunction with my involvement with the IIA.

This submittal includes general comments, followed by comments that align with the questions in the Exposure Draft, and/or the order of the Exposure Draft.

Independent Private Sector Audits (IPSAs): The GAO should acknowledge the use of GAGAS for private sector audits, and applicability of performance standards to those audits. The GAO should provide consideration to firms conducting private sector audits (conflict minerals, and/or otherwise), including suitable flexibility.

> Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") addressed "conflict minerals" in the supply chain of publicly-traded companies. Per the statute's requirement, the SEC promulgated rules, which required companies to conduct due diligence and make annual submittals to the SEC. If filers elected to conclude they manufacture at least one product that is "DRC Conflict Free", they are required to procure and submit an IPSA. The IPSA must be done using GAGAS, and may be conducted by a CPA (using attestation standards) or a non-CPA (using performance standards). The SEC allowed use of non-CPAs as a mechanism to foster competition; in addition, the two specified audit objectives are both process-oriented – for which performance standards are well-suited. In the third year of filings, approximately one-third of the companies that submitted an IPSA used non-CPA firms to do so.
>
> As of July 2017, this is the only submittal of its type that uses GAGAS – but it is a precedent for others, and could come into widespread use during the next five years. The Sustainability Accounting Standards Board completed publication of provisional disclosure standards for environmental, social, and governance (ESG) risks for all sectors and industries (79 in all) in 2016. SASB published the "State of Disclosure Report" in 2016, documenting the general state of disclosures [in Management Discussion & Analysis sections of Forms 10-K] across hundreds of companies. SASB launched a tool in late 2016 that provides analysis of these disclosures to investors with a few clicks. The growing visibility on ESG disclosures, the ready availability of investor-quality information for comparative analysis, and the continued growth in assets under management (AUM) that screen for ESG aspects, it stands to reason that investors will want these disclosures to be trustworthy. These disclosures are not

subject to assurance by financial auditors.

The Congressional and SEC approach for conflict minerals IPSAs is readily applicable. Many ESG disclosures concern processes, management systems, programs, and statements regarding steps taken. These echo the conflict minerals IPSA objectives: in simple terms, the auditor must gain comfort in the design of a due diligence program, and that there is sufficient support for statements made. Private sector companies are much more likely to consider assurance if they are provided with options. The GAGAS performance standards are a useful model for assurance.

Numbering System: Consider using a numbering scheme to differentiate between the requirements an application guidance. For example, an application guidance paragraph could be referred to with "-AG" after the paragraph number (3.39-AG, etc.).

The exposure draft combines requirements and application guidance into a single document. This differentiates between required and suggested practices as one reads the document. It is common practice to provide citations to paragraph numbers in planning documents, work papers, or correspondence. There is no mechanism for a reader viewing such a citation to know whether the paragraph is a requirement or application guidance.

Section 1.23 – Terms: This section is a useful collection of "terms used in GAGAS" – although it is not described as "Definitions." Suggestions for this paragraph include:

- Audit, Internal Audit: "Internal Audit" generally reports to those charged with governance, and has responsibilities and authority to assess any/ all aspects of operations, compliance, reporting, or strategy. The IIA has published a white paper describing Internal Audit's role as a "third line of defense." There are many other activities that function as a "second line of defense." Organizations conduct audits of higher-risk areas, such as environmental, safety, IT security, physical security, quality, etc. These 2LOD functions report to management. Using the Exposure Draft lexicon, they could be considered an internal control. There are many different management frameworks, auditing systems and credentials (ISO among them). Internal Audit has assurance responsibilities over 2LODs, yet practices and effectiveness vary widely. As written, the Exposure Draft uses only "audit." Consider adding a term here to describe these focused, 2LOD auditing activities – and/or making specific mention of them in describing internal controls.
- Deficiency: This term is described at 5.101. Consider adding these to 1.23.
- Significant, or Significant Deficiency: Described at 5.102; consider adding to 1.23.

Question 5 (Chapter 4); Competence and CPE

Competence for Roles (Paragraph 4.10): Consider changing "Entry Level" to "Task Implementation and Basic Management" or adding another category to reflect effort performed on audit teams.

"Entry level" (subparagraph a) connotes a level in the hierarchy of an organization, not the types of things that are done. Entry level auditors can perform tasks other than those listed in the Exposure Draft – including tasks that do not obviously fall into any of the three categories listed. For example, staff with nominal experience can schedule interviews, track audit tasks and progress, and perform other basic project management activities.

Questions 6 and 7: Quality Control and Peer Review

Paragraph 5.63 – External Peer Review General Requirements: Use of performance standards [only] for independent private sector audits is still nascent, but is likely to grow. There are aspects of Government Audit Standards that may not readily apply to IPSAs. I have suggested [in-person meeting at the Conflict Free Sourcing Initiative conference in November 2016, and via email shortly thereafter] that GAO convene a suitable, respected community of practice to review this, and to

publish suitable guidance for this growing need. The External Peer Review is one area that warrants consideration. Provide that an External Peer Review continues as application guidance for firms that conduct only private sector audits, and that use only performance standards.

Paragraph 5.64, 5.66, 5.87, and 5.80 – 5.113 – Selection of Peer Reviewers: Peer reviewers should provide transparency that is similar to that required by the audit firms and government entities. Firms or individuals who conduct external peer reviews should make this information publicly-available, via their websites or other suitable mechanism [such as are described in Paragraph 5.113 et seq]. Firms or individuals who conduct external peer reviews should make the reports they publish available to the public, using the same mechanisms.

> The organizations listed in 5.64 have core teams that provide peer reviews. Other organizations that manage auditors in respected, widespread use may not. For some that do, they are not permitted to conduct a review – let alone sign such a review – using the credential from that auditing body. Simplify the peer review requirements.

5.70 Peer Review Ratings and 5.98 Peer Review Report Ratings: Clarify the meanings of "deficiency" and "significant deficiency"– or use different terms that convey the severity of the difference in terms understandable to non-auditors. Align the definitions with the report ratings. For example, the rating of "pass with deficiency" should correspond to peer reviewers' findings of significant deficiencies, and not gaps that are "improvement opportunities" or otherwise minor (see also Paragraph 9.24).

> The terms "deficiency" and "significant deficiency" are described. However, the report ratings do not differentiate between the significance or materiality of the gap noted. These can be matters of professional judgment, and can involve a substantial degree of subjectivity. If auditors and peer reviewers do not agree on this criteria, then the ultimate users of audit reports and the public cannot be expected to, either.

Paragraph 5.100 – Peer Reviewer Aggregation of Findings: Insert provisions similar to Paragraph 9.42 (obtaining reviews of responsible officials) for the audits themselves, to help avoid publication of unsupported or incorrect information.

> This paragraph is a reasonable guide for the peer reviewer's internal practices. Paragraphs 5.106 and 5.107 describe a practice for communication with the Audit Organization (essentially, the auditee, for purposes of the peer review), including if the audit organization does not believe corrective action is necessary. As written, this practice is mentioned only after publication of the peer reviewer's report.

Report Quality (After Paragraph 9.08 or thereabouts): Retain the "Report Quality Elements" listed at A7.02 in the 2011 edition of GAGAS.

Douglas Hileman, CRMA, CPEA, FSA, P.E.
www.douglashileman.com