June 12, 2023

Mr. Travis Hall
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

RE: Docket No. NTIA–2023–0005
AI Accountability Policy Request for Comment

Dear Mr. Hall:

We appreciate the opportunity to share our views in response to the National Telecommunications and Information Administration (NTIA) request for comment on Artificial Intelligence (AI) system accountability measures and policies (Docket No. 230407–0093). Our views incorporate our long-standing experience as a global leader in audit and assurance services on varied subject matters, such as financial statements, certifications of internal control systems, and sustainability, as well as technological, economic, and statistical data.

From our experience, the established financial reporting ecosystem provides a valuable skeleton and helpful scaffolding for the key components needed to establish an AI accountability framework. Robust US capital markets rely on quality financial reporting that has been achieved through the collective work of a high-functioning ecosystem of players, including management, auditors, standard setters, and regulators. Confidence in the information disclosed by companies — enhanced by independent, third-party assurance — is a critical component of efficient capital markets. Notably, however, the ecosystem around financial reporting is a child of crisis: the stock market crash of 1929 created the initial requirements for reporting by and audits of public companies while the high-profile collapse of companies such as Enron in the early 2000s led to enhanced responsibilities for management to provide reporting around internal control over financial reporting.

We can learn from these experiences by acting decisively to establish the ecosystem around trusted AI, averting a crisis before it has the opportunity to develop. We firmly believe that the federal government needs to move quickly and proactively to establish mechanisms to prevent market and other potentially more harmful systemic failures. Given the rapid pace of technological development, we believe immediate updates to public policy are needed.

As the NTIA notes, AI systems hold substantial promise and, at the same time, pose new risks. In the appendix, we detail recommendations and observations focusing on the mitigation of risks through oversight from regulators and implementation of other aspects of an AI accountability ecosystem modeled on financial reporting. But even the most advanced AI ecosystem can only hope to reduce the risk of harm; there will continue to be risks in the AI lifecycle that extend past the point of existing definitions of control. We believe these unresolved risks can be partially managed by transparency and corporate responsibility to provide end-users with information about the operation of AI for its intended purpose.

Public and private sector cooperation

We support the NTIA's initiative to evaluate a public policy solution to address the risks AI-assisted products and services pose to their users and society. While markets have incentives to create solutions to problems on their own, such market-based solutions often have limitations. For example, voluntary financial statement audits were a market solution to investors' demand for reliable financial information,

but inconsistency and lack of rigor led to the formation of the Securities and Exchange Commission and related regulation to mandate audits for public companies. Similarly, coordination among different parties in the AI ecosystem (e.g., AI providers, auditors, users) and related audits and disclosures will not occur solely in response to market forces. Regulators have established processes and are able to quickly and efficiently respond to emerging developments that may threaten the capital markets or public health and welfare. Although regulators and others in the public sector therefore should be leaders in the AI space, they need to act in concert with other interested parties. Cooperation with the private sector will allow realization of the substantial promise of AI systems to enhance economic competitiveness, create business value, and help address pressing societal issues while mitigating the risks of digital asymmetry, bias, and risks to health and human safety.

Third-party assurance

We believe that third-party assurance related to AI systems will play a unique role in the context of accountability mechanisms given the trust potential, particularly when performed by independent and objective practitioners. We recognize that such assurance engagements represent one AI accountability mechanism among others, but believe they are nevertheless a vital component of a functioning AI assurance ecosystem as they have the ability to enhance confidence in the performance of other participants in the ecosystem.

We know that information that is subject to third-party assurance garners more trust than information provided by a single source. We believe that the highest level of trust in AI systems would be provided by organizations that have:

- **expertise** in the technical operations and algorithms of AI systems development and deployment coupled with extensive training and experience in attestation methodologies performed in accordance with generally accepted risk management frameworks,
- **professional licensure requirements** that mandate the achievement of educational and technical competency and continuing professional education, and
- **a regulator** with the authority to establish professional requirements and assess performance against those requirements.

As discussed in the appendix, public sector regulations should determine how many of the above requirements are necessary to mitigate the assessed level of risk and whether elements of assurance can be built into their existing oversight frameworks.

* * * * *

The appendix includes our observations and recommendations by section of the request for comment. We would be pleased to discuss our comments or answer any specific questions as the NTIA is developing its report principally focused on the AI assurance ecosystem. Please contact Wes Bricker at wesley.bricker@pwc.com, Jennifer Kosar at jennifer.kosar@pwc.com, or Tim Persons at tim.persons@pwc.com.

Sincerely,

PricewaterhouseCoopers LLP

PricewaterhouseCoopers LLP

Appendix

AI ACCOUNTABILITY OBJECTIVES

Purpose of AI accountability mechanisms (questions 1 and 2)

As with building trust in financial information, we believe trust in Artificial Intelligence (AI) systems and the data that feeds them may ultimately be achieved through a two-pronged system: (1) a management assertion on compliance with the applicable trustworthy AI standard or framework and (2) third-party assurance on management's assertion. We believe the combination of these elements would enhance trust, helping AI to be used safely and effectively at scale to realize its full potential.

Management reporting

The first tier of assurance needs to come from those developing the AI system algorithm (i.e., the software consuming the data and updating itself for the next or future use). One of the central features of AI is that the system continuously learns from the data it consumes and changes over time — ideally for the better, but at times for the worse. Since the AI updates itself without human intervention, the developers need to have a process to ensure that AI — fed by sufficient and reliable data — produces results that are within an expected range of acceptable outcomes. Management also needs to ensure that developers are following an established testing protocol.

Making a management certification or assessment public encourages confidence as (1) it evidences management's focus and accountability on the trustworthiness of its AI, and (2) is prepared on the basis of internal control processes.

Role of third-party assurance

Although management ultimately has responsibility for the reliability of its company's AI, external confidence in management information on any topic — from financial reporting, to sustainability, to cybersecurity, to AI — is greatly enhanced when those assertions are subject to third-party assurance.

External evaluations provide an objective and independent validation on management's data and disclosures and may be accomplished in many ways. The work conducted by certified public accountants (CPAs) in accordance with the standards issued by the American Institute of Certified Public Accountants (AICPA), International Auditing and Assurance Standards Board (IAASB), and Public Company Accounting Oversight Board (PCAOB) are referred to as attestations, audits, or reviews (as defined further in our response to question 8), and are designed to enhance the reliability of information by expressing a conclusion or opinion on that information or on management's assertion with respect to that information.

The National Telecommunications and Information Administration (NTIA) has asked whether the structure, credentials, or communication of audits or assessments are impacted depending on whether they are "used to verify a claim, verify compliance with legal standards, or assure compliance with non-binding trustworthy AI goals."[1] Audits or attestation engagements may be structured to compare reported statements to most types of standards, whether those standards are a matter of law, management design, or voluntary goals established by regulatory or other agencies. Certain types of engagements, like attestations performed using the standards of the AICPA, may only be performed by a CPA. The communication or report on the results of these engagements, regardless of who performs them, should specify, among other disclosures, the type of assurance provided, the scope of the procedures, and the framework under which it was performed.

[1] Department of Commerce, NTIA, "AI Accountability Policy Request for Comment," Federal Register Vol. 88, No. 71 (April 13, 2023): 22438.

We believe that third-party assessments should be performed by someone with expertise in both the subject matter and assurance. In fact, 81% of US respondents to our 2021 global investor survey indicated that assurance providers should have expertise in the subject matter and in providing assurance (see our response to question 18). In particular, independent public accounting firms have the requisite skills and experience to use the same core principles applied to financial statement and controls audits to provide assurance on AI systems and data. They also are versed in an interdisciplinary approach that leverages the knowledge of the mathematical and computer sciences (e.g., specialists such as data engineers, statisticians, actuaries, software developers), and therefore have expertise in both AI systems and attestation procedures.

Definitions (question 8)

Just as the ongoing policy debate about the specific definition of "trustworthy AI" may obfuscate the societal imperative to establish recognized standards enabling public reliance on these rapidly evolving tools, the lack of clear definitions of the potential components of an accountability framework — much less the definition of accountability itself — may complicate development of AI accountability policy.

Therefore, we agree that establishing specific definitions of relevant terms is important to promote a shared understanding by all stakeholders. Further, we recommend leveraging existing definitions to the extent possible. Such consistency is important as certain words have a very specific meaning in the context of reporting and deviations may result in misunderstanding and confusion by users of the AI accountability outputs.

Accountability

As discussed above, accountability is both the objective of an AI assurance ecosystem and — together with other characteristics — a component of how it conveys trustworthiness. Accountability has many definitions, but most fundamentally it refers to the act of taking responsibility. This plain English explanation is consistent with the Merriam-Webster dictionary, which defines accountability, in part, as "an obligation or willingness to accept responsibility or to account for one's actions."[2] The Oxford Reference dictionary also frames accountability in the context of responsibility, defining it, in part as, "The requirement for representatives to … accept (some) responsibility for failure, incompetence, or deceit."[3] Finally, the focus on responsibility dovetails with the statement in the Request for Comment that "real accountability can only be achieved when entities are held responsible for their decisions."[4]

Thus, we believe that the paramount purpose of an AI accountability policy is to ensure that a company or other party deploying an AI system is held responsible within the context of a trustworthy AI framework (as discussed in our response to questions 12 and 13). Further, assessments, assurance, and other tools for evidencing accountability aid in holding the applicable parties responsible by evaluating compliance with established frameworks and providing visibility to regulators and other stakeholders as to the degree of compliance.

Assurance

The terms assurance and audit are often used interchangeably and informally, although these words have specific meaning in certain contexts, including work performed over financial statements and sustainability reporting.

Although in common parlance, "assurance" is an expression of confidence or certainty, assurance services generally refer to work performed by a certified public accountant. As described by the AICPA, assurance services reduce uncertainty "by having an independent professional provide a service to enhance the

[2] Merriam-Webster.com Dictionary, Accountability, accessed June 8, 2023.
[3] Oxford University Press, Oxford Reference online, Accountability, accessed June 8, 2023.
[4] NTIA request for comment, 22434.

degree of decision-maker confidence in the information."[5] As discussed under "Audits and reviews," levels of assurance vary depending on the form of engagement; the level required may be determined by regulation or agreement, by management and the auditor, or may incorporate input from the users of the report.

The stated purpose of the request for comment is "to draft and issue a report on AI accountability policy development, focusing especially on the AI assurance ecosystem."[6] A key consideration in developing this policy will be determining the requisite qualifications for the parties providing assurance. Further, to the extent the ultimate policy permits AI accountability engagements to be performed by parties other than certified public accountants, it may be appropriate to reference an "AI accountability ecosystem" in lieu of referring to assurance.

Audits and reviews

The term "audit" should be used with specific meaning. As discussed in guidance from the AICPA, an "audit of financial statements" provides:

> Financial statement users with an opinion by the auditor on whether the financial statements are presented fairly, in all material respects, in accordance with an applicable financial reporting framework, which enhances the degree of confidence that intended users can place in the financial statements. An audit conducted in accordance with [generally accepted auditing standards] and relevant ethical requirements enables the auditor to form that opinion.[7]

An audit opinion is the strongest level of assurance issued by a certified public accountant and it is the level of service that engenders the greatest degree of trust. It is not, however, absolute: as noted in the auditing standards, "absolute assurance is not attainable because of the nature of audit evidence and the characteristics of fraud."[8]

Auditing standards also provide for a form of negative assurance, referred to as a review, in which an auditor "express[es] a conclusion about whether [it] is aware of any material modifications that should be made to the subject matter in order for it to be in accordance with (or based on) the criteria, or the assertion, in order for it to be fairly stated."[9]

The term "audit" can also be used informally. We are aware, for example, that some non-CPA entities currently conduct "AI audits," which may encompass a wide variation in the nature, timing, or extent of procedures performed. Use of the term "audit" without reference to a generally accepted body of standards fails to convey the level of effort applied, the scope of procedures performed, the level of assurance provided over the findings, or the qualifications of the provider, among other shortcomings.

We recommend that any AI accountability policy provide clear guidance on forms of engagement, standards to be applied, and reporting for AI accountability service providers other than certified public accountants.

Assessments

Assessments often refer to work performed by management (and their experts) over their own systems. And, within the context of AI, we believe an assessment is a tool management may use to evaluate its internal processes and staff performance compared to established protocols designed to support an AI system's trustworthiness. Such an assessment may have details regarding the procedures performed, and

---

[5] AICPA, Assurance Services: A white paper for providers and users of business information, 3.
[6] NTIA request for comment, 22433.
[7] AICPA, AU-C Section 200, Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards, paragraph 4.
[8] PCAOB, AS 1015, Due Professional Care in the Performance of Work, paragraph 10.
[9] AICPA, AT-C Section 210, Review engagements, paragraph 3.

the results of those procedures. In addition, internal audit may play an important role in testing over AI systems, aiding management in their assessment process. Further, the ultimate results of an internal assessment may support management's confidence in its own ability to assert that the AI system is trustworthy. Their work may also help inform the procedures performed by an independent third party.

Other terms

Other terms used to refer to some form of work over an AI system may include "verified" or "certified." And, the dictionary definition of the word verify suggests that it may be relevant in establishing a reporting framework (i.e., "to establish the truth, accuracy, or reality of").[10] Likewise, the definitions of certify appear relevant, including "to attest authoritatively: such as (a) confirm … (c) to attest as being true or as represented or as meeting a standard."[11]

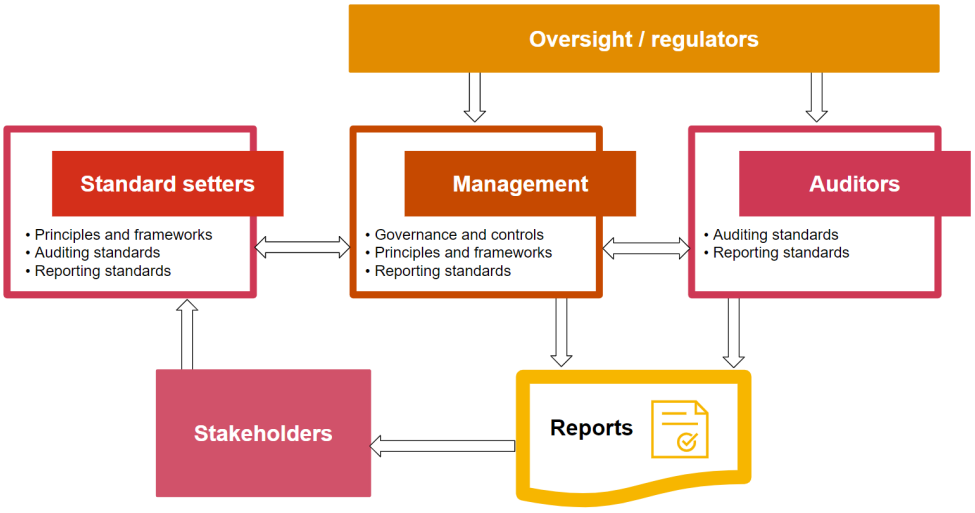
As currently used in the context of AI reporting, however, these terms have no standard meaning and may be applied to a wide array of engagements. This lack of clarity fosters confusions and may contribute to an attitude of distrust, rather than trust, in AI systems. Therefore, as mentioned above, we recommend that the AI accountability policy establish and define standard terms for AI accountability engagements.

EXISTING RESOURCES AND MODELS

Other models (questions 12 and 13)

In developing an AI accountability framework, we recommend that policy makers look to the financial reporting ecosystem as the gold standard in ensuring the reliability of, and market confidence in, company-specific information. The financial markets trade and rely on the information reported, enabled by trust in the clear roles and responsibilities of each of the parties — ranging from regulators, standard setters, investors, companies, and third-party auditors. The emerging sustainability ecosystem is leveraging the baseline established by financial reporting and we recommend that policymakers also emulate this model in support of the trusted and sustainable use of AI.

We believe an AI accountability framework modeled off the key parties and core attributes that contribute to the strength of the financial reporting ecosystem would include the following:



[10] Merriam-Webster.com Dictionary, Verify, accessed June 8, 2023.
[11] Merriam-Webster.com Dictionary, Certify, accessed June 8, 2023.

Attributes of the key components are further described below. In addition, a summary of the necessary frameworks, with linkage to the financial reporting analogue, is included in our response to question 24.

Principles of trusted AI

The starting point for AI accountability is the principles for trusted AI. Although numerous frameworks have been developed, with varying definitions of the characteristics of trustworthy AI, the key attributes are generally encompassed in the National Institute for Standards and Technology (NIST), *Artificial Intelligence Risk Management Framework*, which describes trustworthy AI as "valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with harmful bias managed."[12] In establishing the baseline for measuring AI accountability, we recommend that the NTIA consider these attributes as minimum principles for trusted AI.

Management

The processes required to support the accuracy of AI begin with a sound control environment. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework was established in 1992 as a principles-based approach for companies to exercise oversight in designing, implementing, and conducting internal control that can be applied at the entity, operating, and functional levels.[13] It includes five components — control environment, risk assessment, control activities, information and communication, and monitoring activities — and provides a means to identify and analyze risks, and to develop and manage appropriate responses.[14] The COSO Framework is used by most companies in designing their internal control over financial reporting but it also may be applied to other compliance objectives. As such, COSO or a similar framework should be applied by companies and their boards in the governance of AI activities.

As part of their controls, management should implement organizational practices that provide effective oversight throughout the development lifecycle, recognizing the unique characteristics of AI systems. As a foundation for safe, effective, and equitable AI, management should be able to demonstrate:

- **Organizational governance** – Appropriate governance structures and related processes to manage the risk associated with the use of AI in business functions, considering the core principles of effective governance: (1) demonstration of the importance of integrity and ethical values; (2) assignment of clear roles and responsibilities; and (3) compliance with relevant laws, regulations, standards, and risk management frameworks.
- **Data governance and quality** – Accountability for the data used in model development and system operations, including assessing whether such data is reliable, consistent, unbiased, secured, properly sourced and usable. Data governance and quality standards should incorporate how data is used in AI-related activities to address processes, policies, roles, metrics, and standards that define who has authority and control over data assets and how they may be used.
- **Performance assessment** – Measurement of system operations and algorithmic performance to (1) provide timely insight as to outcomes achieved as compared to design objectives, (2) initiate corrective action as needed, and (3) provide information to those responsible for oversight and monitoring activities. Entities should consider how AI design processes will demonstrate that business and technical performance requirements for AI systems were established prior to development and reference these requirements in the evaluation of a system.
- **Continuous monitoring** – Oversight of dynamic and changing AI system performance over time to track inputs of data, outputs generated from predictive or generative models, and performance parameters. Deficiencies should be resolved promptly based on whether the results

[12] NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, page 12.
[13] COSO, Internal Control – Integrated Framework: Executive Summary, 1.
[14] Ibid., 4–5.

are as expected and in accordance with applicable laws, regulations, policies, and programmatic objectives.

Companies will also need to be specific about how they are addressing risks of AI, based on an agreed-upon trusted AI framework (as discussed above). We analogize the attributes to financial statement assertions, which represent the attributes of financial reporting (e.g., accuracy, existence, completeness). In the financial reporting ecosystem, accounting standards established by the Financial Accounting Standards Board and International Accounting Standards Board detail the principles that ensure these assertions are achieved. The AI accountability ecosystem would also need to develop principles that would allow management to objectively determine whether the attributes have been realized. For example, an AI attribute common to most frameworks is that the results produced by an AI system should be "fair." Principles will need to be developed to ensure that what constitutes "fair" is commonly understood by parties across the ecosystem.

Auditors

Given the vital role that third-party assurance will play in the AI assurance ecosystem, one of the greatest barriers to AI accountability is the lack of a standard accountability reporting framework.

The financial reporting and sustainability ecosystems rely on high-quality audit standards promulgated by the AICPA, IAASB, and PCAOB. The core tenets of generally accepted auditing standards should be leveraged to create a robust set of standards that can be tailored to the specific risks inherent in AI systems. Independent public accounting firms are subject to standards from the PCAOB, AICPA, and IAASB that prescribe the elements of quality control that are essential to the effective design, implementation, and maintenance of firm systems. While the specific requirements of each body's quality control standards differ slightly, they address such topics as firm independence (the concept of being free from any obligation to or interest in the client), integrity and objectivity, leadership responsibilities for quality within the firm (the tone at the top), relevant ethical requirements, acceptance and continuance of client relationships and specific engagements, human resources, engagement performance, and monitoring.

As discussed above, third-party assurance enhances trust. Public company auditors possess (1) expertise in information systems and assurance methodology according to generally accepted standards, (2) robust licensure requirements, and (3) an independent regulator (the Public Company Accounting Oversight Board). These attributes combine to credential public company auditors to provide a high level of assurance and substantially enhance trust. Other parties providing assurance may not have a formal regulator or may lack expertise in either the subject matter or the applied assurance methodology. Further, auditors are practiced in exercising professional skepticism. The AICPA defines professional skepticism as "an attitude that includes a questioning mind and a critical assessment of audit evidence."[15] In applying professional skepticism, auditors gather and objectively evaluate audit evidence by considering the competency and sufficiency of the evidence. Professional skepticism is a skill without which the achievement of a functioning system of financial assurance is not possible. By extension, a system of AI assurance necessarily should incorporate this foundational concept in its structure.

While external assurance is intended to promote trust for external stakeholders, it also gives management objective, independent evidence regarding its own systems and processes. In connection with an audit of the financial statements, the auditors communicate with management and those charged with governance about qualitative aspects of the entity's significant accounting policies, accounting estimates, and financial statement disclosures. Auditors may also communicate observations about the design or operation of the company's internal controls and other matters. And, as we saw with the advent of third-party assurance on a management's audit of internal control over financial reporting, companies are more diligent in their assessments and documentation when there is an expectation of review by an auditor. Therefore, we

[15] AICPA, AU Section 230, Due Professional Care in the Performance of Work, paragraph 7.

believe there is and will remain a clear and present need for risk-contextualized third-party assurance on management's assessment of its internal control over AI systems.

In considering what type of assurance should be built into existing regulatory requirements, public sector agencies should consider the degree of risk of harm and specify the type of assurance provider appropriate to mitigate that risk to an acceptable level.

ACCOUNTABILITY SUBJECTS

AI in the value chain (question 15)

AI applications function as a holistic system of interdependent parts, and are built to evolve and learn based on their contexts. One of the complexities of the AI value chain is the vast array of parties involved — many with overlapping roles — including entities that broker and process raw data, AI solutions providers and consultants, cloud service providers, platform providers, research institutions, organizations, and front-line users. Further, failures that result in outcomes that are inconsistent with the original intent of the system may occur at any point, potentially due to actions taken — or not taken — by any of the parties in the value chain or, perhaps more ominously, by the system itself. Much has been reported about the dangers of AI, from the potentially harmful consequences of misinformation and disinformation to blatant examples of bias. These outcomes are not always traceable to a single person or single algorithm or single point in time. Effective AI accountability, therefore, needs to address the salient risk across the entire value chain.

When entities work together to develop, deploy, and maintain an AI system, each party needs to be accountable for its contribution to the integrity and accuracy of the AI output. A model for this type of multi-nodal responsibility exists in the financial reporting ecosystem today: service organizations (e.g., payroll processors, securities market pricing providers, and cloud enterprise resource planning system providers) process inputs from and provide outputs to users. In many cases, these outputs directly impact the user entity's financial reporting. To support the reliability and integrity of the data provided, service organizations issue a report describing their processes and controls. These reports, however, explicitly acknowledge the interrelationship between the controls of the service organization and the end user, by highlighting complementary controls "that management of the service organization assumes, in the design of [its system], will be implemented by user entities and are necessary to achieve the control objectives."[16]

This convention clearly delineates the controls that are the responsibility of each party, resulting in a transfer of trust from party to party. Further, both management's financial statements and the processes performed by a service organization are typically subject to third-party assurance by CPAs. Service organization reporting — and the related third-party assurance — allows management of the end user to assess the reliability of the information received from the service organization, ultimately supporting management's ability to certify its responsibility for its financial information. Similar concepts are also applicable to reporting in areas highly relevant to the transfer of trust in AI, including security, confidentiality, privacy, processing integrity, and availability.

These models may provide a helpful conceptual framework for applying ownership and accountability across the lifecycle of a given AI system in certain circumstances.

Accountability mechanisms and the AI lifecycle (questions 16 and 17)

The NIST AI risk management framework describes the AI lifecycle in seven stages: planning and design, collection and processing of data, building and training the model, verifying and validating the model, deployment, operation and monitoring, and use of the model/impact from the model.[17] Each part of the

[16] AICPA AT-C Section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting, paragraph 8.
[17] NIST, AI Risk Management Framework: Second Draft, August 18, 2022, Figure 2, page 6.

lifecycle may be controlled or significantly influenced by different entities. For example, a company leveraging AI in its manufacturing process may be involved in the planning and design of the system, as well as the collection of data, but may not build and train the model or may outsource the deployment.

Notwithstanding which party in the value chain is responsible, the first step in performing an effective audit is a risk assessment. The nature, timing, and extent of procedures performed in an audit are designed based on an assessment of the risk of material misstatement. A risk assessment is made in the context of a company's organizational structure, operating environment, macroeconomic conditions, the nature of its business, and numerous other factors. Financial auditors go beyond mere compliance with a predetermined set of specific procedures and instead apply a tailored audit plan that is responsive to the risks identified in the end-to-end process (e.g., understanding transaction initiation, authorization, processing, recording, and reporting).

Although an AI system may be inherently more complex than a financial ledger, the benefits of identifying the key risks through obtaining an end-to-end understanding is equally — if not more — critical. Further, we believe that third-party assurance can add value at various points in the AI lifecycle, including before and after system deployment:

- Third-party assurance obtained before a system is deployed can mitigate risks before negative outcomes occur.
- Third-party assurance obtained after deployment can address risks of unintended and unforeseen results that occur once the AI system is interacting with inputs and data beyond the training set.

We further believe that ongoing assessments after deployment should be performed more frequently than annually, with the precise interval determined based on factors such as the degree to which the AI system relies on static algorithms or is self learning. For certain applications, continuous assessment may be most appropriate. Continuous evaluation will require the development of new auditing technologies that withstand the complexities of assessing a deep neural network or foundation model.

Assurance reporting (question 18)

As discussed in question 30, we believe that businesses, consumers, and other parties impacted by the decisions and results of AI are entitled to know whether and how it is being used.

Further, we recommend mandatory disclosure of third-party assurance or an explanation that no AI accountability work has been performed. Enhanced transparency around AI's use — and its relative trustworthiness — may advance public trust and understanding. The extent of internal testing and certification or third-party assurance should be determined by the applicable regulator and scaled on a continuum based on an assessment of the risk of harm that may result from misinformation or disinformation.

ACCOUNTABILITY INPUTS AND TRANSPARENCY

Records, information, and data quality (questions 20, 21, and 22)

A core tenet of auditing is the requirement to "design[] and perform[] audit procedures to *obtain sufficient appropriate audit evidence* … whether obtained from audit procedures or other sources, that is used by the auditor in arriving at the conclusions on which the auditor's opinion is based" (emphasis added).[18] Factors considered in assessing the sufficiency and appropriateness of audit evidence include the risk of material misstatement, the quality of evidence obtained, and whether it is relevant and reliable. Further, although audit evidence includes information obtained from outside the company for corroboration, the company's records are the starting point for any audit.

[18] PCAOB AS 1105, Audit Evidence, paragraphs 1 and 2.

Similarly, AI accountability procedures will require sufficient, appropriate evidence, necessitating access to a variety of records, data, and other documentation related to the system including:

- Information about the organization's governance structure and broader control environment, including roles and responsibilities
- Description of the development process, algorithm, architecture, and configuration of the model, as well as the design of controls in each respective aspect of the system
- Data used to train the system and consumed by the system in its operational state
- Documentation of any pre-processing steps applied to the training data
- Documentation of the system's compliance with legal, regulatory, and ethical specifications
- Results of testing performed throughout the development process and during the subject period
- Design and results of any recalibration performed during the period
- Information about the design of controls to detect emergent properties and bugs

This list may appear daunting, particularly given the nature of AI which, in some ways, may create an obstacle to retention of sufficient documentation to support accountability. Traditional automation is explainable through the rules outlined by the human designer (i.e., the underlying business requirements and program code). And, the related documentation of this type of system is relatively static, enabling rigorous testing and oversight. In contrast, an AI model may have the ability to adjust its own rules, morphing and evolving without human intervention. Further, in some cases, one or both of what an AI system is inferring from the data and/or how it is modifying its algorithm may be unclear — one of the key facets of AI that leads to headlines like, "How Could A.I. Destroy Humanity?"[19]

To address the risks inherent in AI and to enable appropriate oversight, testing, and monitoring, management needs to be able to document the data used, identify changes made to the algorithm (including changes, if any, made of the system's own accord), and explain how the results were derived. This visibility, however, may be challenging in the case of a dynamic AI system given potential difficulties in reproducing the underlying algorithm. Subjecting this type of system to an accountability process will require extensive documentation and a means to identify the exact configuration of the system at a point in time.

Maintaining a robust trail of an AI system's algorithm is decidedly challenging, and some may argue that the need to do so may limit entrepreneurial AI development and may prove to be a disincentive for obtaining third-party assurance. But relying on the results of an AI system without some type of assurance risks reliance on unsupported AI with unforeseen consequences. Despite the challenge, management will need to be confident in an AI system's inputs, processes, and outputs, which may require the development of new protocols or technologies.

Document retention

Gaps in information supporting AI systems — whether inadequate, incomplete, inaccessible, or incomprehensible — create a significant barrier to AI assurance. Thus, record retention requirements are a foundational element of an AI accountability framework, notwithstanding potential challenges given the nature of AI.

This imperative, however, is not new or unique to AI. Retention of relevant records is already an intrinsic aspect of business operations in the United States; companies are subject to a vast web of documentation retention rules promulgated by federal, state, and local governments. These existing rules provide a helpful baseline for the establishment of requirements to support an AI assurance ecosystem. For example, Securities and Exchange Commission (SEC) rules require companies to maintain certain financial books and records and to retain them until at least the applicable statute of limitations on enforcement has lapsed (generally five to ten years depending on the violation).[20] And, most, if not all

[19] The New York Times, web edition, June 10, 2023.
[20] 15 U.S. Code §78m (b)(2), Books, records, and internal accounting.

organizations are subject to Internal Revenue Service (IRS) rules which require taxpayers to "keep [their] business records available at all times for inspection by the IRS," with length of retention guidelines generally ranging from three to seven years.[21]

In many ways, the purpose of AI document retention is similar to that of financial business records, suggesting that the retention requirements of the SEC and IRS may be an appropriate starting point. Other federal rules and regulations, however, may also have a nexus to AI systems. For example, depending on their nature, the data, algorithms, and outputs of AI systems may be subject to regulations stemming from a myriad of Federal laws such as the Americans with Disabilities Act, the Civil Rights Act of 1964, the Fair Labor Standards Act, the Health Insurance Portability and Accountability Act, and the Occupational Safety and Health Act. AI record retention requirements should necessarily contemplate this broader legal and regulatory context and align, as applicable, with other existing rules and regulations.

Requirements for service providers

As noted, we believe companies should be required to maintain sufficient records for an adequate period of time to support AI accountability engagements. This documentation will also be important for companies' own quality control processes, compliance with laws and regulations, supporting public disclosures, and transparency, as well as to ensure that the AI results are traceable and explainable.

We believe it is equally important to establish requirements for the documentation prepared by the assurance provider to support its AI accountability engagement (i.e., workpapers). Sufficient documentation prepared in accordance with professional standards is an inextricable element of audits of financial statements as described in the "Background and Basis for Conclusions" to PCAOB Auditing Standard (AS) No. 3, *Audit Documentation*:

> The [PCAOB's] standard on audit documentation is one of the fundamental building blocks on which both the integrity of audits and the Board's oversight will rest. The Board believes that the quality and integrity of an audit depends, in large part, on the existence of a complete and understandable record of the work the auditor performed, the conclusions the auditor reached, and the evidence the auditor obtained that supports those conclusions.[22]

Engagements performed in accordance with the standards of the AICPA and IAASB are also subject to workpaper documentation requirements.[23] Further, the audit standards setters, as well as the SEC, specify retention requirements for auditors.[24] Certified public accountants may also be subject to the documentation and retention requirements of state licensing boards.

While the evidentiary requirements for auditors are well established, other service providers performing AI accountability engagements may not consistently exercise similar discipline in preparing and retaining documentation. Therefore, we believe establishing formal documentation and retention requirements is an important element of an effective AI accountability framework. The auditing standards may provide a useful starting point in establishing these requirements. See further discussion in the "Existing Resources and Models" section.

Reporting of audit results (question 23)

Users rely on a standard audit report to understand whether the financial statements are fairly stated in all material respects. Standardized reporting provides users with an instant shorthand regarding the

---

[21] Internal Revenue Service website, Publication 583, and Topic No. 305, Recordkeeping, accessed June 7, 2023.
[22] PCAOB AS 3, Audit Documentation, Background and Basis for Conclusions, paragraph A4.
[23] AICPA, AU-C Section 230, Audit Documentation; IAASB, International Standard on Auditing 230, Audit Documentation.
[24] AICPA, AU-C Section 230, Audit Documentation; IAASB, International Standard on Auditing 230, Audit Documentation; PCAOB AS 1215, Audit Documentation; and, SEC, Regulation S-X, Item 210.02-06.

reliability of the financial information. This type of comfort is even more critical in emerging areas like AI and sustainability where stakeholders may lack foundational knowledge of the subject matter or the related disclosure requirements. In our global investor survey completed in fall 2021, 77% of US respondents report having more trust in ESG information if it has been assured.[25] Further, almost as many US investors (72%) believe ESG metrics should be assured at the same level as the financial statements (i.e., reasonable assurance).[26] We believe that stakeholders would similarly look to assurance on AI information to enhance trust.

Assurance alone, however, is not enough. Instead, to maximize and optimize its value, an audit report needs to be readily available — and instantly recognizable — to stakeholders. It may be relatively easy to make an audit report available through existing sharing mechanisms such as public posting on websites, although laws and regulations would be needed to require this type of disclosure (see question 30). That said, users of AI would need to know to look for proof of assurance. Different delivery mechanisms, or a way to denote whether a system has been subjected to third-party assurance, would need to be developed ideally with visibility at the point of initial interaction with an AI-enabled system.

Further, comprehensibility will be diminished in a landscape of bespoke reporting, where reports are tailored to each individual engagement. Standardized reporting — including references to the agreed trustworthy AI framework, elucidation of the evaluation criteria, and articulation of findings — would help engender public trust. Importantly, the level of assurance provided should be clear and the scope of work performed, as well as the findings, if any, should be easily understandable by non-technical experts.

Further, we believe that the form of report should be standardized across industries and stakeholder groups. Superficially, disparate public reporting of "AI accountability 'products'" depending on industry or stakeholders may appear to provide greater clarity.[27] We believe, however, that additional detail and complexity would only serve to confuse the ongoing public debate. Company reporting is the appropriate location for elaboration, if needed. The accountability results should emulate the long-established reporting on financial statement results with standard, sector-agnostic reports, differentiated only by the level of assurance provided.

BARRIERS TO EFFECTIVE ACCOUNTABILITY

Barriers to AI accountability (question 24)

The principal current barrier to AI accountability is the lack of commonly accepted standards for any of the parties to the AI ecosystem. To achieve the opportunity provided by AI — without catastrophic consequences for society — the private and public sectors need to move rapidly to advance the nationwide adoption of a standard trustworthy AI framework, together with the supporting accountability and reporting standards.

The standards needed to achieve a robust AI accountability system include:

Standards	Description	Financial reporting analogue
Trusted AI framework	Operational standards for companies and parties employing AI	General commercial regulations (e.g. antitrust, corruption, consumer protection, intellectual property, environmental, occupational health and safety)

[25] PwC's US investor survey: The economic realities of ESG
[26] Ibid.
[27] NTIA request for comment, 22440.

Standards	Description	Financial reporting analogue
AI reporting standards	Requirements for external reporting	US Generally Accepted Accounting Principles or International Financial Reporting Standards
AI internal control standards	Control requirements for companies employing AI in their own operations or interfacing with external customers	COSO Integrated Framework
Accountability reporting framework	Standards for accountability reporting engagements, including minimum quality control and reporting requirements	Auditing standards promulgated by the AICPA, IAASB, or PCAOB

In addition, the financial reporting ecosystem includes regulatory oversight from the PCAOB and SEC as well as requirements implemented by the stock exchanges and other parties to the financial markets (e.g., banking regulators). These oversight bodies require adherence to reporting and other requirements while also providing a check on compliance by all parties to the ecosystem. The lack of AI laws and regulations requiring adherence to specified standards, reporting, and audits is a further impediment to creation of an environment of true AI accountability. Thus, establishment of similar regulatory oversight over use of AI is another crucial element in forming true AI accountability.

Each of the crucial components in a high functioning AI accountability ecosystem is further discussed in the "Existing Resources and Models" section. As previously noted, however, development of the financial reporting ecosystem occurred in response to crisis and developed over a long period of time. Regulators now need to move rapidly to develop a robust ecosystem capable of balancing the competing objectives of harnessing the potential power of AI while containing potential abuses.

In many ways, lack of time may be the biggest obstacle to effective accountability given challenges inherent in developing these multiple frameworks. We recommend leveraging existing frameworks from financial reporting as an important first step and welcome the opportunity to work with regulators in establishing principles and guidelines. Further, we believe that the federal government has a crucial role in corralling AI, as further discussed in our response to question 30.

AI ACCOUNTABILITY POLICIES

Focus of AI accountability regulation (question 30)

We believe AI accountability is best driven through public policy initiatives at the federal level to drive enactment of laws and regulations over the use of AI. Swift action is needed to develop a supporting set of cohesive requirements delineating the responsibilities of all parties to the AI accountability ecosystem, including companies, auditors, regulators, and potentially standard setters. Further, we recommend that the NTIA look to the gold standard of reporting and accountability set by the financial reporting ecosystem as a baseline in creating the multiple frameworks needed. Detail on the components needed to establish a high-functioning ecosystem are included in our response to the "Existing Resources and Models" section and further highlighted in the "Barriers to Effective Responsibility" section.

Public and private sector cooperation

There are numerous instances in which users may be unaware that the information on which they are relying was generated by AI. To encompass all potential areas of risk, public agencies need to work

collaboratively with the private sector (e.g., companies, standard setters, non-governmental organizations, accounting firms and other service providers). No one organization working in isolation has the ability to scope this issue, identify potential solutions, and establish a comprehensive AI accountability framework and supporting standards. Any AI accountability standards developed also need to fit seamlessly into existing oversight mechanisms, allowing regulatory and other compliance entities to respond in a manner befitting the assessed risk of harm from AI within their particular sphere of influence.

Cooperation among governmental agencies and other stakeholders would provide the benefit of multiple perspectives and deep subject matter expertise — allowing more rapid and informed progress. For example, in addition to developing the trustworthy AI framework and related auditing and reporting standards, regulators will need to solve an array of issues, ranging from establishing oversight to determining whether different AI applications warrant different levels of internal or external assessment. Leveraging the knowledge of those most informed about a sector's salient risks will aid in progressing these initiatives.

User notification

Even with relatively rapid action, however, development of standards able to keep pace with technology innovation will take time. As an immediate intervening step to protect the American public, we believe regulations should be enacted requiring comprehensive notification to direct users and any potentially impacted parties about the use of AI. The notification should provide information including: the purpose of the AI, whether results are subject to any human oversight (e.g., are results of a cancer scan initially read by AI reviewed by a radiologist before sharing with the patient?), and how the AI reacts to missing data (i.e., does it make up information to fill gaps?). Developing a comprehensive list of relevant requirements, identifying notification mechanisms, and enacting legislation to require prominent disclosure should be a priority.

Uniformity of AI accountability requirements (question 34)

Multiple parties globally are actively developing various voluntary and mandatory frameworks for responsible AI. Individual companies, non-profit entities, and other interested parties are also developing their own proprietary frameworks intended to establish trust. This fragmented landscape contributes to the lack of clear agreement on the common risks and principles associated with AI. In turn, this splintering of requirements and various competing frameworks exponentially complicates compliance by all parties in the ecosystem, risking defeating their purpose of "giving affected parties (including customers, investors, affected individuals and communities, and regulators) confidence that the technologies are in fact worthy of trust."[28]

Thus, we support development and implementation of a federal AI accountability policy and related laws and regulations in an effort to establish consistent minimum practices across the US. Many of the civil rights, civil liberties, and privacy protections that currently exist in the US stem from federal law and regulation (e.g., anti-discrimination, workplace safety, fraud and defamation), which further supports implementing nationwide requirements to address the potential for harm of AI systems to these protections. In addition, AI systems may operate across state lines, also supporting the need for the primary regulations to be promulgated by the federal government.

Individual states may also choose to develop incremental AI-related laws within their specific jurisdictions. Competing state laws create significant challenges for companies as well as other stakeholders given the exponential complexity in ensuring compliance. The risk of disparate frameworks will increase in the absence of federal action. We believe an optimal solution would be for the federal government to move quickly to establish minimum standards, potentially forestalling conflicting action by

[28] NTAI request for comment, 22435.

individual states. This will drive greater accuracy and reliability of results while likely minimizing the incremental costs.

Consistency within the US is not the only priority: we support international coordination and harmonization to the extent possible. Disparate approaches internationally are likely to diminish the benefits to be derived from AI accountability measures, particularly given the multinational nature of many AI systems. US AI-related laws, however, also need to reflect the rights provided to citizens that may not exist universally (e.g., freedom of speech). Therefore, although we believe a universal set of global standards should be the goal, fostered by global coordination and collaboration, we recognize that individual jurisdictions may need to reflect their local environment. In such cases, interoperability should be preserved to the extent possible.