determines that there are no more than minor changes in the activities, the mitigation and monitoring measures would remain the same and appropriate, and the findings in the initial IHA remain valid.

Dated: April 7, 2023.
Kimberly Damon-Randall,
Director, Office of Protected Resources,
National Marine Fisheries Service.

[FR Doc. 2023–07729 Filed 4–12–23; 8:45 am]
BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration
[Docket No. 230407–0093]
RIN 0660–XC057
AI Accountability Policy Request for Comment

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice, request for Comment.

SUMMARY: The National Telecommunications and Information Administration (NTIA) hereby requests comments on Artificial Intelligence (“AI”) system accountability measures and policies. This request focuses on self-regulatory, regulatory, and other measures and policies that are designed to provide reliable evidence to external stakeholders—that is, to provide assurance—that AI systems are legal, effective, ethical, safe, and otherwise trustworthy. NTIA will rely on these comments, along with other public engagements on this topic, to draft and issue a report on AI accountability policy development, focusing especially on the AI assurance ecosystem.

DATES: Written comments must be received on or before June 12, 2023.

ADDRESSES: All electronic public comments on this action, identified by Regulations.gov docket number NTIA–2023–0005, may be submitted through the Federal e-Rulemaking Portal at www.regulations.gov. The docket established for this request for comment can be found at www.regulations.gov. NTIA–2023–0005. Click the “Comment Now!” button to complete the required fields, and enter or attach your comments. Additional instructions can be found in the “Instructions” section below after “Supplementary Information.”

FOR FURTHER INFORMATION CONTACT: Please direct questions regarding this Notice to Travis Hall at thall@ntia.gov with “AI Accountability Policy Request for Comment” in the subject line, or if by mail, addressed to Travis Hall, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW, Room 4725, Washington, DC 20230; telephone: (202) 482–3522. Please direct media inquiries to NTIA’s Office of Public Affairs, telephone: (202) 482–7002; email: press@ntia.gov.

SUPPLEMENTARY INFORMATION:

Background and Authority

Advancing trustworthy Artificial Intelligence (“AI”) is an important federal objective. The National AI Initiative Act of 2020 2 established federal priorities for AI, creating the National AI Initiative Office to coordinate federal efforts to advance trustworthy AI applications, research, and U.S. leadership in the development and use of trustworthy AI in the public and private sectors. Other legislation, such as the landmark CHIPS and Science Act of 2022, also support the advancement of trustworthy AI. These initiatives are in accord with Administration efforts to advance American values and leadership in AI and technology platform accountability 3 and to promote “trustworthy artificial intelligence” as part of a national security strategy.

5 See, e.g., CHIPS and Science Act of 2022, Pub. L. 117–167, 136 Stat. 1392 (Aug. 9, 2022) (providing support and guidance for the development of safe, secure, and trustworthy AI systems, including considerations of fairness and bias as well as the ethical, legal, and societal implications of AI more generally).
6 Supra note 2 (implemented though the National Artificial Intelligence Initiative, https://ai.gov (last visited Jan. 19, 2023)).
8 White House, Biden-Harris Administration’s National Security Strategy (Oct. 12, 2022) at 21, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (last visited Feb. 1, 2023) (identifying “trusted artificial intelligence” and “trustworthy artificial intelligence” as Endeavors that further AI system governance to combat harmful bias and promote equity and inclusion also support the Administration’s agenda on racial equity and support for underserved communities. Moreover, efforts to advance trustworthy AI are core to the work of the Department of Commerce. In recent public outreach, the International Trade Administration noted that the Department “is focused on solidifying U.S. leadership in emerging technologies, including AI” and that the “United States seeks to promote the development of innovative and trustworthy AI systems that respect human rights, [and] democratic values, and are designed to enhance privacy protections.”
9 To advance trustworthy AI, the White House Office of Science and Technology Policy produced a Blueprint for an AI Bill of Rights (“Blueprint”), providing guidance on “building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy.” The National Institute of Standards and Technology (NIST) produced an AI Risk Management Framework, which provides a voluntary process for managing a wide range of potential AI risks. Both of these initiatives

9 Dated: April 7, 2023.
12 International Trade Administration, Request for Comments on Artificial Intelligence Export Competitiveness, 87 FR 50288, 50288 (Oct. 17, 2022) (“ITA is broadly defining AI as both the goods and services that enable AI systems, such as data, algorithms and computing power, as well as AI-driven products across all industry verticals, such as autonomous vehicles, robotics and automation technology, medical devices and healthcare, security technology, and professional and business services, among others.”).

contemplate mechanisms to advance the trustworthiness of algorithmic technologies in particular contexts and practices.\textsuperscript{1,2} Mechanisms such as measurements of AI system risks, impact assessments, and audits of AI system implementation against valid benchmarks and legal requirements, can build trust. They do so by helping to hold entities accountable for developing, using, and continuously improving the quality of AI products, thereby realizing the benefits of AI and reducing harms. These mechanisms can also incentivize organizations to invest in AI system governance and responsible AI products. Assurance that AI systems are trustworthy can assist with compliance efforts and help create marks of quality in the marketplace.

NTIA is the President’s principal advisor on telecommunications and information policy issues. In this role, NTIA studies and develops policy on the impacts of information and communications technology on civil rights;\textsuperscript{3} transparency in software components;\textsuperscript{4} and the use of emerging digital technologies.\textsuperscript{5} NTIA’s statutory authority, its role in advancing sound internet, privacy, and digital equity policies, and its experience leading stakeholder engagement processes align with advancing sound policies for trustworthy AI generally and AI accountability policies in particular.

**Definitions and Objectives**

Real accountability can only be achieved when entities are held responsible for their decisions. A range of AI accountability processes and tools (e.g., assessments and audits, governance policies, documentation and reporting, and testing and evaluation) can support this process by proving that an AI system is legal, effective, ethical, safe, and otherwise trustworthy—a function also known as providing AI assurance.

The term “trustworthy AI” is intended to encapsulate a broad set of technical and socio-technical attributes of AI systems such as safety, efficacy, fairness, privacy, notice and explanation, and availability of human alternatives. According to NIST, “trustworthy AI” systems are, among other things, “valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy-enhanced, and fair with their harmful bias managed.”\textsuperscript{16} Along the same lines, the Blueprint identifies a set of five principles and associated practices to help guide the design, use, and deployment of AI and other automated systems. These are: (1) safety and effectiveness, (2) algorithmic discrimination protections, (3) data privacy, (4) notice and explanation, and (5) human alternatives, consideration and fallback.\textsuperscript{17} These principles align with the trustworthy AI principles propounded by the Organisation for Economic Co-operation and Development (OECD) in 2019, which 46 countries have now adopted.\textsuperscript{18} Other formulations of principles for responsible or trustworthy AI containing all or some of the above-stated characteristics are contained in industry codes,\textsuperscript{19} academic writing,\textsuperscript{20} civil society codes,\textsuperscript{21} and guidance and frameworks from standards bodies,\textsuperscript{22} and other governmental instruments.\textsuperscript{23} AI assurance is the practical implementation of these principles in applied settings with adequate internal or external enforcement to provide for accountability.

Many entities already engage in accountability around cybersecurity, privacy, and other risks related to digital technologies. The selection of AI and other automated systems for particular scrutiny is warranted because of their unique features and fast-growing importance in American life and commerce. As NIST notes, these systems are “trained on data that can change over time, sometimes significantly and unexpectedly, affecting system functionality and trustworthiness in ways that are hard to understand. AI systems and the contexts in which they are deployed are frequently complex, making it difficult to detect and respond to failures when they occur. AI systems are inherently socio-technical in nature, meaning they are influenced by societal dynamics and human behavior. AI risks—and benefits—can emerge from the interplay of technical aspects combined with societal factors related to how a system is used, its interactions with other AI systems, who operates it, and the social context in which it is deployed.”\textsuperscript{24}
The objective of this engagement is to solicit input from stakeholders in the policy, legal, business, academic, technical, and advocacy arenas on how to develop a productive AI accountability ecosystem. Specifically, NTIA hopes to identify the state of play, gaps, and barriers to creating adequate accountability for AI systems, any trustworth AI goals that might not be amenable to requirements or standards, how supposed accountability measures might mask or minimize AI risks, the value of accountability mechanisms to compliance efforts, and ways governmental and non-governmental actions might support and enforce AI accountability practices.

This Request for Comment uses the terms AI, algorithmic, and automated decision systems without specifying any particular technical tool or process. It incorporates NIST’s definition of an “AI system,” as “an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments.” This Request’s scope and use of the term “AI” also encompasses the broader set of technologies covered by the Blueprint: “automated systems” with “the potential to meaningfully impact the American public’s rights, opportunities, or access to critical resources or services.”

Accountability for Trustworthy AI

1. Growing Regulatory Interest in AI Accountability Mechanisms

Governments, companies, and civil society organizations are developing AI governance tools to mitigate the risks of autonomous systems to individuals and communities. Among these are accountability mechanisms to show that AI systems are trustworthy, which can help foster responsible development and deployment of algorithmic systems, while at the same time giving affected parties (including customers, investors, affected individuals and communities, and regulators) confidence that the technologies are in fact worthy of trust. Governments around the world, and within the United States, are beginning to require accountability mechanisms including audits and assessments of AI systems, depending upon their use case and risk level. For example, there are relevant provisions in the European Union’s Digital Services Act requiring audits of very large online platforms’ systems, the draft EU Artificial Intelligence Act requiring conformity assessments of certain high-risk AI tools before deployment, and New York City Law 144 requiring bias audits of certain automated hiring tools used within its jurisdiction. Several bills introduced in the U.S. Congress include algorithmic impact assessment or audit provisions. In the data and consumer protection space, policies focus on design features of automated systems by requiring in the case of privacy-by-design, or prohibiting in the case of “dark patterns,” certain design choices to secure data and consumer protection. Governments are mandating accountability measures for government-deployed AI systems. Related tools are also emerging in the private sector from non-profit entities such as the Responsible AI Institute (providing system certifications) to startups and well-established companies, such as Microsoft’s Responsible AI Standard and Datasheets for Datasets, the Rolls-Royce Aletheia Framework, Google’s Model Card Toolkit, and many others. Federal regulators have been addressing AI system risk management in certain sectors for more than a decade. For example, the Federal Reserve in 2011 issued SR–11–7 on Algorithmic Model Risk to produce impact assessments for the Federal Trade Commission.

2. See, e.g., Council Regulation 2016/679, of the European Parliament and of the Council on Apr. 27, 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 25 (implementing data protection by design principles).

3. See, e.g., Cal. Civ. Code § 1798.140, subd. (l), (h) (effective Jan. 1, 2023) (regulating the use of a “dark pattern” defined as a “user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation” and noting that “agreement obtained through use of dark patterns does not constitute consent.”


Management, noting that reducing risks requires “critical analysis by objective, informed parties that can identify model limitations and produce appropriate changes’’ and, relatedly, the production of testing, validation, and associated records for examination by independent parties. As financial agencies continue to explore AI accountability mechanisms in their areas, other federal agencies such as the Equal Employment Opportunities Commission have begun to do the same. Moreover, state regulators are considering compulsory AI accountability mechanisms.

2. AI Audits and Assessments

AI systems are being used in human resources and employment, finance, health care, education, housing, transportation, law enforcement and security, and many other contexts that significantly impact people’s lives. The appropriate goal and method to advance AI accountability will likely depend on the risk level, sector, use case, and legal or regulatory requirements associated with the system under examination. Assessments and audits are among the most common mechanisms to provide assurance about AI system characteristics. Guidance, academic, and regulatory documents use the terms “assessments” (including risk, impact, and conformity) and “audits” in various ways and without standard definition.46

Often in these references, “assessment” refers to an entity’s internal review of an AI system to identify risks or outcomes. An “audit” often refers to an external review of an AI system at a point in time to assess performance against accepted benchmarks. Assessments and audits may both be conducted on a continuous basis, and may be conducted either by internal or external reviewers.

Common areas of focus for AI audits and assessments include harmful bias and discrimination, effectiveness and validity, data protection and privacy, and transparency and explainability (how understandable AI system predictions or decisions are to humans). For information services like social media, large language and other generative AI models, and search, audits and assessments may also cover harms related to the distortion of communications through misinformation, disinformation, deep fakes, privacy invasions, and other content-related phenomena.

Audits may be conducted internally or by independent third parties. An internal audit may be performed by the team that developed the technology or by a separate team within the same entity. Independent audits may range from “black box” adversarial audits conducted without the help of the audited entity to “white box” cooperative audits conducted with substantial access to the relevant models and processes. Audits may be made public or given limited circulation, for example to regulators. They may be conducted by professional experts or undertaken by impacted lay people.50

While some audits and assessments may be limited to technical aspects of a particular model, it is widely understood that AI models are part of larger systems, and these systems are embedded in socio-technical contexts. How models are implemented in practice could depend on model interactions, employee training and recruitment, enterprise governance, stakeholder mapping and engagement,51 human agency, and many other factors.52 The most useful audits and assessments of these systems, therefore, should extend beyond the technical to broader questions about governance and purpose. These might include whether the people affected by AI systems are meaningfully consulted in their design 53 and whether the choice to use the technology in the first place was well-considered.54

Some accountability mechanisms may use legal standards as a baseline. For


example, standards for employment discrimination on the basis of sex, religion, race, color, disability, or national origin may serve as benchmarks for AI audits, as well as for legal compliance actions. Civil society groups are developing additional operational guidance based on such standards. Some firms and startups are beginning to offer testing of AI models on a technical level for bias and/or disparate impact. It should be recognized that for some features of trustworthy AI, consensus standards may be difficult or impossible to create.

3. Policy Considerations for the AI Accountability Ecosystem

Among the challenges facing policymakers in the AI accountability space are tradeoffs among trustworthy AI goals, barriers to implementing accountability mechanisms, complex AI lifecycle and value chains, and difficulties with standardization and measurement.

Accountability ecosystems that might serve as models for AI systems range from financial assurance, where there are relatively uniform financial auditing practices, to environmental, social, and governance (ESG) assurance, where standards are quite diverse. Considering the range of trustworthy AI system goals and deployment contexts, it is likely that at least in the near term, AI accountability mechanisms will be heterogeneous. Commentators have raised concerns about the validity of certain accountability measures. Some audits and assessments, for example, may be scoped too narrowly, creating a “false sense” of assurance. Given this risk, it is important that those performing AI accountability tasks are sufficiently qualified to provide credible evidence that systems are trustworthy.

There may be other barriers to providing adequate and meaningful accountability. Some mechanisms may require datasets built with sensitive data that puts privacy or security at risk, raising questions about trade-offs among different values. In addition, there may be insufficient access to the subject system or its data, insufficient qualified personnel to conduct and/or inadequate audit or assessment standards to benchmark the work.

Timing is another complication for AI accountability, and especially for providing assurance of AI systems. The point in an AI system lifecycle at which an audit or assessment is conducted, for example, will impact what questions it answers, how much accountability it provides, and to whom that accountability is offered. The General Services Administration has described an AI lifecycle that starts with pre-design (e.g., problem specification, data identification, use case selection), progresses through design and development (e.g., model selection, training, and testing), and then continues through deployment. Other federal agencies use substantially similar lifecycle schema. Throughout this lifecycle, dynamic interactions with data and iterative learning create many moments for evaluation of specific model and the AI system as a whole.

The AI value chain, including data sources, AI tools, and the relationships among developers and customers, can also be complicated and impact accountability. Sometimes a developer will train an AI tool on data provided by a customer, or the customer may in turn use the tool in ways the developer did not foresee or intend. Data quality is an especially important variable to examine in AI accountability. A developer training an AI tool on a customer’s data may not be able to tell how that data was collected or organized, making it difficult for the developer to assure the AI system. Alternatively, the customer may use the tool in ways the developer did not foresee or intend, creating risks for the developer wanting to manage downstream use of the tool. When responsibility along this chain of AI system development and deployment is fractured, auditors must decide whose

---


data and which relevant models to analyze, whose decisions to examine, how nested actions fit together, and what is within the audit’s frame.

Public and private bodies are working to develop metrics or benchmarks for trustworthy AI where needed. Standards-setting bodies such as IEEE and ISO, as well as research organizations focusing on measurements and standards, notably NIST, are devising technical standards that can improve AI governance and risk management and support AI accountability. These include standards for general technology process management (e.g., risk management), standards applicable across technologies and applications (e.g., transparency and anti-bias), and standards for particular technologies (e.g., emotion detection and facial recognition). For some trustworthy AI goals, it will be difficult to harmonize standards across jurisdictions or within a standard-setting body, particularly if the goal involves contested moral and ethical judgements. In some contexts, not deploying AI systems at all will be the means to achieve the stated goals.

To address these barriers and complexities, commentators have suggested that policymakers and others can foster AI accountability by: mandating impact assessments and auditing, defining “independence” for third-party audits, setting procurement standards, incentivizing effective audits and assessments through bounties, prizes, and subsidies, creating access to data necessary for AI audits and assessments, creating consensus standards for AI assurance, providing auditor certifications, and making test results available for use. We particularly seek input on these policy proposals and mechanisms.

Instructions for Commenters:

Through this Request for Comment, we hope to gather information on the following questions. These are not exhaustive, and commenters are invited to provide input on relevant questions not asked below. Commenters are not required to respond to all questions. When responding to one or more of the questions below, please note in the text of your response the number of the question to which you are responding. Commenters should include a page number on each page of their submissions. Commenters are welcome to provide specific actionable proposals, rationales, and relevant facts.

Please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. All comments received are a part of the public record and will generally be posted to Regulations.gov without change. All personal identifying information (e.g., name, address) voluntarily submitted by the commenter may be publicly accessible.

Questions

AI Accountability Objectives

1. What is the purpose of AI accountability mechanisms such as certifications, audits, and assessments? Responses could address the following:
   a. What kinds of topics should AI accountability mechanisms cover? How should they be scoped?
   b. What are assessments or internal audits most useful for? What are external assessments or audits most useful for?
   c. An audit or assessment may be used to verify a claim, verify compliance with legal standards, or assure compliance with non-binding trustworthy AI goals. Do these differences impact how audits or assessments are structured, credentialed, or communicated?
   d. Should AI audits or assessments be folded into other accountability mechanisms that focus on such goals as human rights, privacy protection, security, and diversity, equity, inclusion, and access? Are there other potential benefits?


70 See, e.g., Nikos Alonos and Maria Xente. Ethics-Based Auditing of Automated Decision-Making Systems: Intervention Points and Policy Implications, AI & Society, 35, 15–21 (Feb. 2022), https://doi.org/10.1007/s10460-021-09893-9 (arguing for investigations of social media algorithms, “[p]olicy makers should consider sponsoring academic-industry partnerships allowing researchers to access this research and the data generated in the process to produce evidence of public value while securing privacy.”)

benchmarks for these other accountability mechanisms that should inform AI accountability measures?

6. The application of accountability measures (whether voluntary or regulatory) is more straightforward for some trustworthy AI goals than for others. With respect to which trustworthy AI goals are there existing requirements or standards? Are there any trustworthy AI goals that are not amenable to requirements or standards? How should accountability policies, whether governmental or non-governmental, treat these differences?

7. Are there ways in which accountability mechanisms are unlikely to further, and might even frustrate, the development of trustworthy AI? Are there accountability mechanisms that unduly impact AI innovation and the competitiveness of U.S. developers?

8. What are the best definitions of and relationships between AI accountability, assurance, assessments, audits, and other relevant terms?

Existing Resources and Models

9. What AI accountability mechanisms are currently being used? Are the accountability frameworks of certain sectors, industries, or market participants especially mature as compared to others? Which industry, civil society, or governmental accountability instruments, guidelines, or policies are most appropriate for implementation and operationalization at scale in the United States? Who are the people currently doing AI accountability work?

10. What are the best definitions of terms frequently used in accountability policies, such as fair, safe, effective, transparent, and trustworthy? Where can terms have the same meanings across sectors and jurisdictions? Where do terms necessarily have different meanings depending on the jurisdiction, sector, or use case?

11. What lessons can be learned from accountability processes and policies in cybersecurity, privacy, finance, or other areas?81

12. What aspects of the United States and global financial assurance systems provide useful and achievable models for AI accountability?

13. What aspects of human rights and/or industry Environmental, Social, and Governance (ESG) assurance systems can and should be adopted for AI accountability?

14. Which non-U.S. or U.S. (federal, state, or local) laws and regulations already requiring an AI audit, assessment, or other accountability mechanism are most useful and why? Which are least useful and why?

Accountability Subjects

15. The AI value or supply chain is complex, often involving open source and proprietary products and downstream applications that are quite different from what AI system developers may initially have contemplated. Moreover, training data for AI systems may be acquired from multiple sources, including from the customer using the technology. Problems in AI systems may arise downstream at the deployment or customization stage or upstream during model development and data training.

a. Where in the value chain should accountability efforts focus?

b. How can accountability efforts at different points in the value chain best be coordinated and communicated?

c. How should vendors work with customers to perform AI audits and/or assessments? What is the role of audits or assessments in the commercial and/or public procurement process? Are there specific practices that would facilitate credible audits (e.g., liability waivers)?

d. Since the effects and performance of an AI system will depend on the context in which it is deployed, how can accountability measures accommodate unknowns about ultimate downstream implementation?

16. The lifecycle of any given AI system or component also presents distinct junctures for assessment, audit, and other measures. For example, in the case of bias, it has been shown that “[b]ias is prevalent in the assumptions about which data should be used, what AI models should be developed, where the AI system should be placed—or if AI is required at all.”82 How should AI accountability mechanisms consider the AI lifecycle? Responses could address the following:

a. Should AI accountability mechanisms focus narrowly on the technical characteristics of a defined model and relevant data? Or should they feature other aspects of the socio-

---

80 See, e.g., Jakob Mokander et al., Auditing Large Language Models: A Three-layered Approach.


82 Reva Schwartz et al., Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, NIST Special Publication 1270, at 6, https://doi.org/10.6028/NIST.SP.1270.
technical system, including the system in which the AI is embedded? When is the narrower scope better and when is the broader better? How can the scope and limitations of the accountability mechanism be effectively communicated to outside stakeholders?

b. How should AI audits or assessments be timed? At what stage of design, development, and deployment should they take place to provide meaningful accountability?

c. How often should audits or assessments be conducted, and what are the factors that should inform this decision? How can entities operationalize the notion of continuous auditing and communicate the results?

d. What specific language should be incorporated into governmental or non-governmental policies to secure the appropriate timing of audits or assessments?

17. How should AI accountability measures be scoped (whether voluntary or mandatory) depending on the risk of the technology and/or of the deployment context? If so, how should risk be calculated and by whom?

18. Should AI systems be released with quality assurance certifications, especially if they are higher risk?

19. As governments at all levels increase their use of AI systems, what should the public expect in terms of audits and assessments of AI systems deployed as part of public programs? Should the accountability practices for AI systems deployed in the public sector differ from those used for private sector AI? How can government procurement practices help create a productive AI accountability ecosystem?

Accountability Inputs and Transparency

20. What sorts of records (e.g., logs, versions, model selection, data selection) and other documentation should developers and deployers of AI systems keep in order to support AI accountability? How long should this documentation be retained? Are there design principles (including technical design) for AI systems that would foster accountability-by-design?

21. What are the obstacles to the flow of information necessary for AI accountability either within an organization or to outside examiners? What policies might ease researcher and other third-party access to inputs necessary to conduct AI audits or assessments?

22. How should the accountability process address data quality and data voids of different kinds? For example, in the context of automated employment decision tools, there may be no historical data available for assessing the performance of a newly deployed, custom-built tool. For a tool deployed by other firms, there may be data a vendor has access to, but the audited firm itself lacks. In some cases, the vendor itself may have intentionally limited its own data collection and access for privacy and security purposes. How should AI accountability requirements or practices deal with these data issues? What should be the roles of government, civil society, and academia in providing useful data sets (synthetic or otherwise) to fill gaps and create equitable access to data?

23. How should AI accountability “products” (e.g., audit results) be communicated to different stakeholders? Should there be standardized reporting within a sector and/or across sectors? How should the translational work of communicating AI accountability results to affected people and communities be done and supported?

Barriers to Effective Accountability

24. What are the most significant barriers to effective AI accountability in the private sector, including barriers to independent AI audits, whether cooperative or adversarial? What are the best strategies and interventions to overcome these barriers?

25. Is the lack of a general federal data protection or privacy law a barrier to effective AI accountability?

26. Is the lack of a federal law focused on AI systems a barrier to effective AI accountability?

27. What is the role of intellectual property rights, terms of service, contractual obligations, or other legal entitlements in fostering or impeding a robust AI accountability ecosystem? For example, do nondisclosure agreements or trade secret protections impede the assessment or audit of AI systems and processes? If so, what legal or policy developments are needed to ensure an effective accountability framework?

28. What do AI audits and assessments cost? Which entities should be expected to bear these costs? What are the possible consequences of AI accountability requirements that might impose significant costs on regulated entities? Are there ways to reduce these costs? What are the best ways to consider costs in relation to benefits?

29. How does the dearth of measurable standards or benchmarks impact the uptake of audits and assessments?

AI Accountability Policies

30. What role should government policy have, if any, in the AI accountability ecosystem? For example: a. Should AI accountability policies and/or regulation be sectoral or horizontal, or some combination of the two?

b. Should AI accountability regulation, if any, focus on inputs to audits or assessments (e.g., documentation, data management, testing and validation), on increasing access to AI systems for auditors and researchers, on mandating accountability measures, and/or on some other aspect of the accountability ecosystem?

c. If a federal law focused on AI systems is desirable, what provisions would be particularly important to include? Which agency or agencies should be responsible for enforcing such a law, and what resources would they need to be successful?

d. What accountability practices should government (at any level) itself mandate for the AI systems the government uses?

31. What specific activities should government fund to advance a strong AI accountability ecosystem?

32. What kinds of incentives should government explore to promote the use of AI accountability measures?

33. How can government work with the private sector to incentivize the best documentation practices?

34. Is it important that there be uniformity of AI accountability requirements and/or practices across the United States? Across global jurisdictions? If so, is it important only within a sector or across sectors? What is the best way to achieve it?

Alternatively, is harmonization or interoperability sufficient and what is the best way to achieve that?
**DEPARTMENT OF DEFENSE**

Department of the Air Force

**Record of Decision for the Foreign Military Sales Pilot Training Center at Ebbing Air National Guard Base, Arkansas, Environmental Impact Statement**

**ACTION:** Notice of Availability of Record of Decision.

**SUMMARY:** On March 11, 2022, the Department of the Air Force (DAF) signed the Record of Decision (ROD) for the Record of Decision for the Foreign Military Sales (FMS) Pilot Training Center at Ebbing Air National Guard (ANG) Base, Arkansas, Environmental Impact Statement.

**ADDRESSES:** Mr. David Martin, AFEC/ CZN, Building 1 Bay 8 Room 8009, 3515 S General McMullen, San Antonio TX 78226–1710, (210) 925–4266; david.martin.127@us.af.mil.

**SUPPLEMENTARY INFORMATION:** The DAF has selected to beddown 12 Royal Singapore Air Force F–16 aircraft and 24 F–35 FMS aircraft at Ebbing ANG Base, Arkansas.

The DAF decision documented in the ROD was based on matters discussed in the Final Environmental Impact Statement, inputs from the public and regulatory agencies, and other relevant factors. The Final Environmental Impact Statement was made available to the public on February 3, 2023, through a Notice of Availability in the Federal Register (Volume 88, Number 23, Page 7445) with a waiting period that ended on March 7, 2023.

**Authority:** This Notice of Availability is published pursuant to the regulations (40 CFR part 1506.6) implementing the provisions of the National Environmental Policy Act (42 U.S.C. 4321, et seq.) and the Air Force’s Environmental Impact Analysis Process (32 CFR parts 989.21(b) and 989.24(b)(7)).

**Tommy W. Lee,**

Acting Air Force Federal Register Liaison Officer.

**BILLING CODE 5001–10–P**

**COMMISSION OF FINE ARTS**

**Notice of Meeting**

Per 45 CFR chapter XXI 2102.3, the next meeting of the U.S. Commission of Fine Arts is scheduled for April 20, 2023, at 9:00 a.m. and will be held via online videoconference. Items of discussion may include buildings, infrastructure, parks, memorials, and public art.

Draft agendas, the link to register for the online public meeting, and additional information regarding the Commission are available on our website: www.cfa.gov. Inquiries regarding the agenda, as well as any public testimony, should be addressed to Thomas Luebke, Secretary, U.S. Commission of Fine Arts, at the above address; by emailing cfastaff@cfa.gov; or by calling 202–504–2200. Individuals requiring sign language interpretation for the hearing impaired should contact the Secretary at least 10 days before the meeting date.

**Dated April 3, 2023 in Washington, DC.**

**Susan M. Raposa,**

Technical Information Specialist.

**BILLING CODE 6330–01–P**

**DEPARTMENT OF EDUCATION**

**[Docket No.: ED–2023–SCC–0023]**

**Agency Information Collection Activities:** Submission to the Office of Management and Budget for Review and Approval; Comment Request; Student Assistance General Provision—Subpart E—Verification Student Aid Application Information

**AGENCY:** Federal Student Aid (FSA), Department of Education (ED).

**ACTION:** Notice.

**SUMMARY:** In accordance with the Paperwork Reduction Act (PRA) of 1995, the Department is proposing an extension without change of a currently approved information collection request (ICR).

**DATES:** Interested persons are invited to submit comments on or before May 15, 2023.

**ADDRESSES:** Written comments and recommendations for proposed information collection requests should be submitted within 30 days of publication of this notice. Click on this link www.reginfo.gov/public/do/PRAMain to access the site. Find this information collection request (ICR) by selecting “Department of Education” under “Currently Under Review,” then check the “Only Show ICR for Public Comment” checkbox. Reginfo.gov provides two links to view documents related to this information collection request. Information collection forms and instructions may be found by clicking on the “View Information Collection (IC) List” link. Supporting statements and other supporting documentation may be found by clicking on the “View Supporting Statement and Other Documents” link.

**FOR FURTHER INFORMATION CONTACT:** For specific questions related to collection activities, please contact Beth Grebeldinger, 202–377–4018.

**SUPPLEMENTARY INFORMATION:** The Department is especially interested in public comment addressing the following issues: (1) is this collection necessary to the proper functions of the Department; (2) will this information be processed and used in a timely manner; (3) is the estimate of burden accurate; (4) how might the Department enhance the quality, utility, and clarity of the information to be collected; and (5) how might the Department minimize the burden of this collection on the respondents, including through the use of information technology. Please note that written comments received in response to this notice will be considered public records.

**Title of Collection:** Student Assistance General Provision—Subpart E—Verification Student Aid Application Information

**OMB Control Number:** 1845–0041

**Type of Review:** An extension without change of a currently approved ICR.

**Respondents/Affected Public:** Private Sector; Individuals and Households; State, Local, and Tribal Governments.

**Total Estimated Number of Annual Responses:** 23,855,169.

**Total Estimated Number of Annual Burden Hours:** 3,835,336.

**Abstract:** This request is for an extension of the information collection supporting the policies and reporting requirements contained in subpart E of part 668—Verification and Updating of Student Aid Application Information. Sections 668.53, 668.54, 668.55, 668.56, 668.57, 668.59 and 668.61 contain information collection requirements (OMB control number 1845–0041). This subpart governs the verification and updating of information provided on the Free Application for Federal Student Aid (FAFSA) which is used to calculate an applicant’s Expected Family Contribution (EFC) for purposes of determining an applicant’s need for student financial assistance under Title IV of Higher Education Act of 1965, as amended (HEA). The collection of this