Testimony

Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

ARTIFICIAL INTELLIGENCE

Key Practices to Help Ensure Accountability in Federal Use of AI

Taka Ariga, Chief Data Scientist, Science, Technology Assessment and Analytics

Highlights of GAO-23-106811, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

May 16, 2023

ARTIFICIAL INTELLIGENCE

Key Practices to Help Ensure Accountability in Federal Use of AI

Why GAO Did This Study

To help managers ensure accountability and the responsible use of AI in government programs and processes, GAO has developed an AI Accountability Framework. Separately, GAO has identified mission-critical gaps in federal workforce skills and expertise in science and technology as high-risk areas since 2001.

This testimony summarizes two related reports—GAO-22-105388 and GAO-21-519SP. The first report addresses the digital skills needed to modernize the federal government. The second report describes discussions by experts on the types of risks and challenges in applying AI systems in the public sector.

To develop the June 2021 AI Framework, GAO convened a Comptroller General Forum in September 2020 with AI experts from across the federal government, industry, and nonprofit sectors. The Framework was informed by an extensive literature review, and the key practices were independently validated by program officials and subject matter experts.

For the November 2021 report on digital workforce skills, GAO convened a roundtable discussion in October 2021 comprised of chief technology officers, chief data officers, and chief information officers, among others. Participants discussed ways to develop a dedicated talent pool to help meet the federal government's needs for digital expertise.

View GAO-23-106811. For more information, contact Taka Ariga, Chief Data Scientist, 202-512-6888, arigat@gao.gov
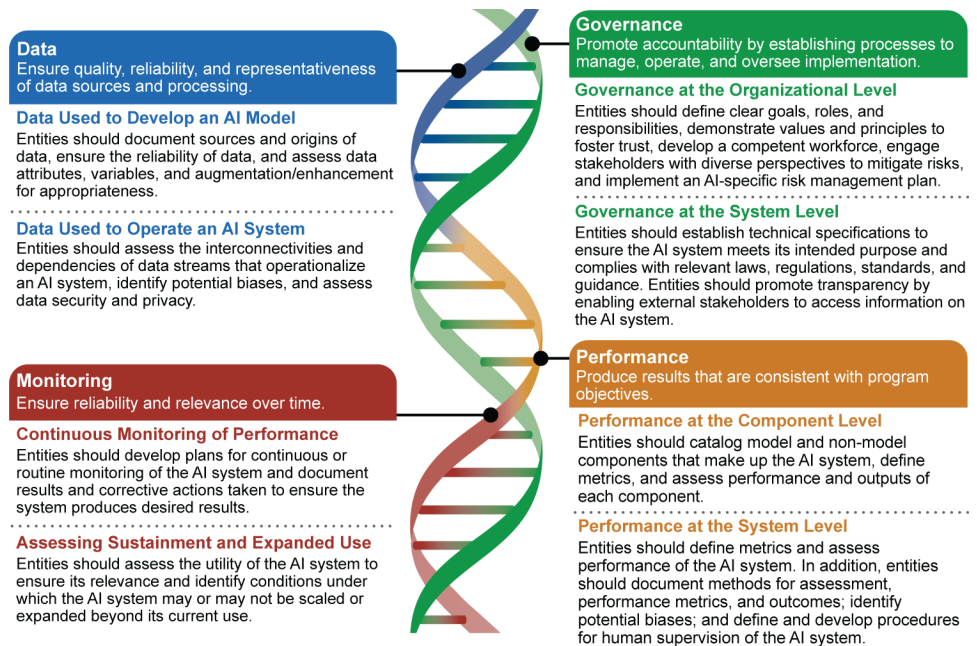
What GAO Found

Artificial intelligence (AI) is evolving at a rapid pace and the federal government cannot afford to be reactive to its complexities, risks, and societal consequences. Federal guidance has focused on ensuring AI is responsible, equitable, traceable, reliable, and governable. Third-party assessments and audits are important to achieving these goals. However, a critical mass of workforce expertise is needed to enable federal agencies to accelerate the delivery and adoption of AI.

Participants in an October 2021 roundtable convened by GAO discussed agencies' needs for digital services staff, the types of work that a more technical workforce could execute, in areas such as artificial intelligence, and challenges associated with current hiring methods. They noted such staff would require a variety of digital and government-related skills. Participants also discussed challenges associated with existing policies, infrastructure, laws, and regulations that may hinder agency recruitment and retention of digital services staff.

During a September 2020 Comptroller General Forum on AI, experts discussed approaches to ensure federal workers have the skills and expertise needed for AI implementation. Experts also discussed how principles and frameworks on the use of AI can be operationalized into practices for managers and supervisors of these systems, as well as third-party assessors. Following the forum, GAO developed an AI Accountability Framework of key practices to help ensure responsible AI use by federal agencies and other entities involved in AI systems. The Framework is organized around four complementary principles: governance, data, performance, and monitoring.

Artificial Intelligence (AI) Accountability Framework

Data
Ensure quality, reliability, and representativeness of data sources and processing.

Data Used to Develop an AI Model
Entities should document sources and origins of data, ensure the reliability of data, and assess data attributes, variables, and augmentation/enhancement for appropriateness.

Data Used to Operate an AI System
Entities should assess the interconnectivities and dependencies of data streams that operationalize an AI system, identify potential biases, and assess data security and privacy.

Governance
Promote accountability by establishing processes to manage, operate, and oversee implementation.

Governance at the Organizational Level
Entities should define clear goals, roles, and responsibilities, demonstrate values and principles to foster trust, develop a competent workforce, engage stakeholders with diverse perspectives to mitigate risks, and implement an AI-specific risk management plan.

Governance at the System Level
Entities should establish technical specifications to ensure the AI system meets its intended purpose and complies with relevant laws, regulations, standards, and guidance. Entities should promote transparency by enabling external stakeholders to access information on the AI system.

Monitoring
Ensure reliability and relevance over time.

Continuous Monitoring of Performance
Entities should develop plans for continuous or routine monitoring of the AI system and document results and corrective actions taken to ensure the system produces desired results.

Assessing Sustainment and Expanded Use
Entities should assess the utility of the AI system to ensure its relevance and identify conditions under which the AI system may or may not be scaled or expanded beyond its current use.

Performance
Produce results that are consistent with program objectives.

Performance at the Component Level
Entities should catalog model and non-model components that make up the AI system, define metrics, and assess performance and outputs of each component.

Performance at the System Level
Entities should define metrics and assess performance of the AI system. In addition, entities should document methods for assessment, performance metrics, and outcomes; identify potential biases; and define and develop procedures for human supervision of the AI system.

Source: GAO. | GAO-23-106811

United States Government Accountability Office

Chairman Peters, Ranking Member Paul, and Members of the Committee:

Thank you for the opportunity to discuss our work on artificial intelligence (AI). My testimony today summarizes two relevant GAO reports: our June 2021 Framework entitled *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*[1] and our November 2021 report on developing a pipeline of federal digital staff, entitled *Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff.*[2]

In our AI Accountability Framework, we highlighted that, given the rapid pace at which AI is evolving, the federal government cannot afford to be reactive to AI's complexities, risks, and societal consequences. GAO's objective was to identify key practices to help ensure accountability and responsible AI use by federal agencies and other entities.[3] Foundational to solving the AI accountability challenge is having a critical mass of digital expertise to help accelerate responsible delivery and adoption of AI capabilities. A talented and diverse cadre of digital-ready federal employees is essential to a government that can effectively design, develop, deploy, use, and monitor AI systems. In our Digital Services report, we noted that, as the federal government continues its modernization efforts, it faces a severe shortage of digital expertise, including in the field of AI. Each federal agency is individually coping with challenges in hiring, managing, and retaining staff with digital services skills because of a limited pipeline of candidates and bureaucratic processes.

Various federal guidance have attempted to guide responsible, equitable, traceable, reliable, and governable AI capabilities. At the same time, robust and independent audits are important to ensuring that these goals are achieved. However, as AI technology advances, responsible management of AI systems will be challenging if the skills necessary to successfully develop,

---

[1]GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities,* GAO-21-519SP (Washington, D.C.: June 30, 2021).

[2]GAO, *Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff,* GAO-22-105388 (Washington, D.C.: Nov. 19, 2021).

[3]The Framework is organized around four complementary principles that address governance, data, performance, and monitoring. For each principle, the Framework describes key practices for federal agencies and other entities that are considering, selecting, and implementing AI systems. Each practice includes a set of questions for entities, auditors, and third-party assessors to consider as well as procedures for auditors and third-party assessors.

buy, or use AI capabilities are lacking. In our AI Accountability Framework, we highlight the need to recruit, develop, and retain competent personnel to ensure accountability and responsible use of AI in government programs and processes.

Our AI Accountability Framework distills insights from cross-sectoral 23 experts convened during the Forum on Artificial Intelligence by the Comptroller General of the United States held on September 9 and 10, 2020. The work for the report also included an extensive literature review and independent validation of key practices from program officials and subject matter experts.[4]

For our Digital Services report, GAO convened a roundtable discussion on October 13, 2021 comprised of chief technology officers, chief data officers, chief information officers, and those in similar roles across the federal government, as well as knowledgeable representatives from academia and nonprofits. Additional information about our scope and methodology can be found in that report.

We performed the work on which this testimony is based in accordance with all applicable sections of GAO's Quality Assurance Framework.

Background

AI Life Cycle

The life cycle of an AI system involves four phases: design, development, deployment, and continuous monitoring.[5] As shown in figure 1, each phase includes considerations articulating the system's concepts, collecting and processing data, building one or more machine learning

---

[4]GAO currently has work underway on federal agencies' efforts and plans related to AI and the Department of Homeland Security's use of AI. We expect to publish the former in fall 2023 and the latter in early 2024.

[5]See OECD, *Artificial Intelligence in Society* (OECD Publishing: Paris, France, revised Aug. 2019), accessed Apr. 4, 2021, https://www.oecd.org/publications/artificial-intelligence-in-society-eedfee77-en.htm Select Committee on Artificial Intelligence of the National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update* (Washington, D.C.: June 2019); and *GAO, Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care,* GAO-21-7SP (Washington, D.C.: Nov. 30, 2020).

models, validating the system, continuously assessing its impact and, if necessary, retiring an AI system from production.[6]

Figure 1: The Phases in the AI Life Cycle

Design involves articulating the system's concept and objectives, underlying assumptions, context and requirements, and potentially building a prototype.

Continuous monitoring involves operating the AI system and continuously assessing its recommendations and impacts (both intended and unintended) in light of objectives and ethical considerations. This phase identifies problems and adjusts by reverting to other phases or, if necessary, retiring the AI system from production.

The Phases in the AI Life Cycle

Development involves planning and design, including establishing technical requirements, data collection and processing, model building and interpretation, and system verification and validation.

Deployment involves piloting, checking compatibility with legacy systems, ensuring regulatory compliance, managing organizational change, and evaluating user experience.

Source: GAO. | GAO-23-106811

Technical and Societal Implications of AI

Implementing AI systems involves assessing technical performance, as well as identifying and mitigating any societal concerns. For example, to manage technical performance, AI technical

---

[6]OECD, *Artificial Intelligence in Society*.

stakeholders—data scientists, data engineers, developers, cybersecurity specialists, program managers, and others—will have to ensure that the AI system solves the problem initially identified; uses data sets appropriate for the problem; selects the most suitable learning algorithms; and evaluates and validates the system and its components to ensure it is functioning as intended. Without such assurances, AI systems may perform in unintended ways or otherwise not achieve the goals set out to achieve. As shown in figure 2, in addition to the AI technical stakeholders noted above, a broader community of participants—policy and legal experts, subject matter experts, and individuals using the AI system or impacted by its use, among others—should be engaged in AI development.

Figure 2: Example of the Community of Stakeholders Engaged in AI Development
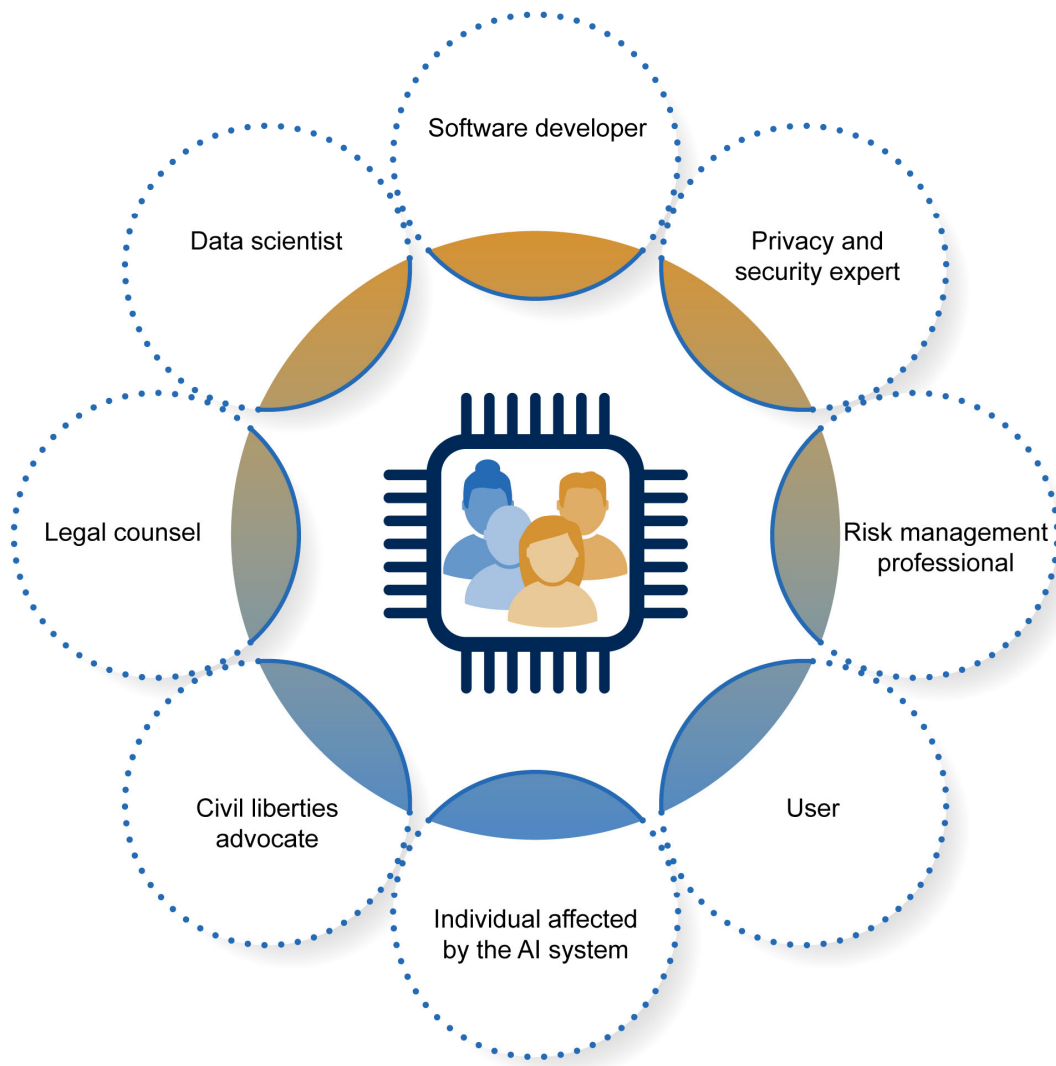
Federal Government Digital Services

Federal agencies rely on digital services to interact with the public and improve organizational performance. Such digital services, as defined by the Office of Management and Budget, include the delivery of digital information (e.g., data or content) and transactional services (e.g., online forms) across a variety of platforms, devices, and delivery mechanisms, such as websites, mobile applications, and social media. The digital services take a variety of forms (see fig. 3).

Figure 3: Examples of Digital Services Skills, Expertise, and Disciplines

Artificial Intelligence
Application development
Cybersecurity and incidence response
User-centric design and digital twins
Data engineering and data science
Data visualization and communication
Robotic process automation
Cloud services and infrastructure modernization
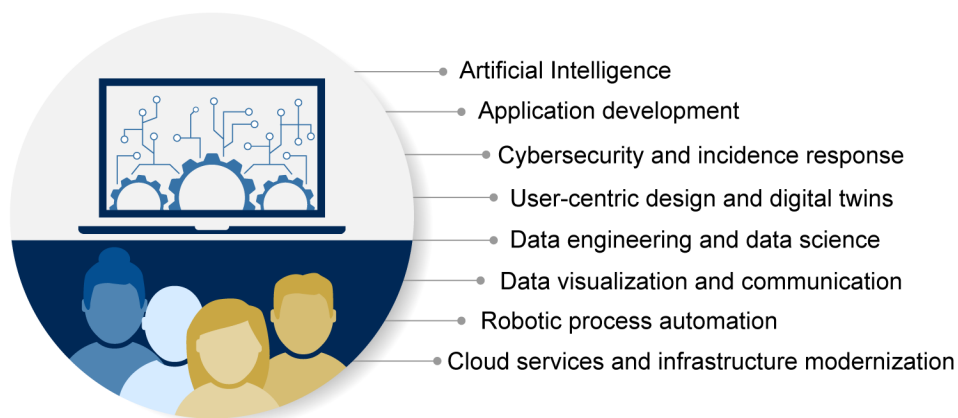
Source: GAO analysis of roundtable participants' perspectives, and industry and government documents (text); GAO (icons). | GAO-23-106811

Individuals can obtain the necessary digital skills through a variety of pathways. For example, they can attend undergraduate and graduate degree programs, certification programs, and digital skills "boot camps," or they can access free online courses and learn on their own. Additionally, some employers provide on-the-job training in areas such as AI, data science, and cloud services. For example, one company we interviewed has established an academy to provide its new digital services employees with a multi-week, in-person training to enhance their skills.

Developing a Federal Digital Workforce Pipeline

Effective use of AI to improve government operations requires a digitally-ready workforce. Since 2001, however, GAO has identified mission-critical gaps in federal workforce skills and expertise

5

in fields such as science, technology, engineering, and mathematics as high-risk areas.[7] Agencies' needs for digital services staff span varying degrees of urgency and roles.

During our October 2021 roundtable discussion, technology leaders and knowledgeable experts shared their perspectives on developing a pipeline of federal digital staff. The discussion included observations about agencies' immediate and long-term needs, key characteristics of a digital services academy, and agency and government-wide considerations around recruitment and retention of digital services staff.

<u>Immediate and Long-Term Needs</u>

Roundtable participants discussed agencies' immediate and long-term needs for digital services staff, the types of inherently governmental work that a digital-ready workforce could execute, and challenges associated with current hiring methods. For example, one roundtable participant noted that their agency had more than 2,000 open positions requiring digital skill sets, and another described numerous project backlogs. Such gaps may lead to cascading implementation challenges.

Additionally, participants said there is a long-term need for in-house talent across roles such as executives, program staff, product managers, software developers, and engineers who understand data architecture and algorithmic elements.

<u>Key Characteristics of a Digital Services Academy</u>

Multiple reports by national advisory groups have suggested that one solution to the lack of digital expertise is that the federal government establish a new service academy—similar to the military academies—to train future civil servants in the digital competencies needed to modernize government (see fig. 4).[8]

---

[7]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[8]The National Security Commission on Artificial Intelligence, *Final Report* (Arlington, VA.: 2021) and The National Artificial Intelligence Advisory Committee, *Year 1 Report* (May 2023).

Figure 4: Example of a Digital Services Academy Concept

A degree-granting institution

Curriculum designed to meet agencies' needs

Students receive specialized training and experience

Graduates perform a term of federal digital service

Source: GAO analysis of roundtable participants' perspectives and government documents (text) and Irina Strelnikova/stock.adobe.com (graphic). | GAO-23-106811

A digital services academy could help develop the pipeline of digital services workers to better meet the needs of the federal workforce, according to roundtable participants. Digital services staff could apply advanced technologies, such as AI in health care, or conduct investigative work using machine learning systems. Roundtable participants noted that digital services staff could also use newer technologies to develop services faster or at a lower cost.

Considerations for such an academy include the kinds of skills that would be taught and the composition and size of a graduating class. Digital services staff would require a variety of both digital and government-related skills to meet agencies' needs. Digital skills include application development, data engineering, and other core AI competencies. Government-related skills include knowing how to navigate the requirements of federal data governance and information assurance regimes. In addition, participants noted that a master's degree pipeline may be more appropriate than an undergraduate degree pipeline because agencies need staff with advanced skills in leading projects and programs, data curation, and digitalization.

A digital services academy composed of a diverse student body may further help address societal impacts. One participant noted that programs may attract a more diverse student body if they have a technical component and a social, mission-driven component. For example, a

course on "responsible data science" would likely attract students who are demographically diverse and interested in mission-driven work.

<u>Agency and Government-wide Considerations</u>

Agencies can prepare for a pipeline of qualified digital services staff by taking steps such as integrating mission needs into digital services projects, developing professional growth opportunities, cultivating institutional relationships, establishing support networks, and building a data-centric culture, according to roundtable participants. At the same time, participants discussed government-wide challenges associated with existing policies, infrastructure, laws, and regulations that may hinder agency recruitment and retention of digital services staff. For example:

- *Modernizing technological infrastructure*. Participants said a lack of modern technology infrastructure limits the ability of government agencies to leverage the skills of digital services staff.

- *Addressing compensation concerns*. Current salaries and compensation for federal digital services staff are not competitive with the private sector.

- *Streamlining the federal hiring process*. Without a more streamlined approach to onboarding staff, many digital services staff would likely not be willing to wait out the lengthy federal hiring process when the private sector can hire more quickly.

Factors Affecting Oversight of AI in the Public Sector

Our AI Accountability Framework emphasizes substantive approaches third-party assessors and auditors should take to develop credible assurance assessments of AI systems. Experts in our forum discussed how principles on the use of AI can be operationalized into practices for managers and supervisors of these systems, as well as third-party assessors. The forum included topics such as governance factors to consider in auditing AI systems, criteria auditors can use in assessing AI systems, issues and challenges in auditing AI systems in the public

sector, and evaluation of AI systems for bias and equity.[9] Participants also highlighted challenges that federal agencies are facing, such as having a need for technical expertise, a limited understanding of how AI makes its decisions, and limited access to key information due to commercial procurement of such systems.

Our AI Accountability Framework is organized around four complementary principles, which address governance, data, performance, and monitoring. For each principle, the framework describes key practices for federal agencies and other entities that are considering, selecting, and implementing AI systems. For example:

- **Governance.** This principle describes key practices to promote accountability by establishing processes to manage, operate, and oversee AI implementation. For example, *Workforce* highlights the importance of recruiting, developing, and retaining personnel with multidisciplinary skills and experience in design, development, deployment, assessment, and monitoring of AI systems.

- **Data.** This principle describes key practices to help entities use data that are appropriate for the intended use of each AI system. For example, *Reliability* emphasizes the need to ensure the reliability of the data used to develop the models.

- **Performance.** This principle describes key practices to help entities produce results that are consistent with program objectives. For example, *Bias* describes the necessity of identifying potential biases, inequities, and other societal concerns resulting from the AI system.

- **Monitoring.** This principle describes key practices to help entities ensure their AI systems remain reliable and relevant over time. For example, *Traceability* discusses how entities will need to document results of monitoring activities and any corrective actions taken to promote traceability and transparency.

---

[9]For more information on topics discussed at the CG Forum such as factors affecting oversight of AI, AI governance, sources of evidence, methods to assess implementation of AI systems, and identifying and mitigating potential bias and inequities, see Appendix II of the Framework.

Additionally, each practice includes a set of questions for entities, auditors, and third-party assessors to consider, as well as procedures for auditors and third-party assessors. For more information on the principles and key practices within the Framework, see Appendix I.

In summary, we noted in our AI Accountability Framework that AI is evolving at a pace at which we cannot afford to be reactive to its complexities, risks, and societal consequences. Auditors and the oversight community play a vital role in the "trust but verify" equation and need a blueprint to evaluate this changing technology.

More importantly, organizations that build, purchase, and deploy AI need a framework to understand how AI systems will be evaluated. In recent years, both foreign and domestic stakeholders have developed governance and auditing frameworks, in part, to address the technical and societal issues associated with using AI in the public sector.

GAO looks forward to seeing our Framework in use by federal agencies, and to working with the oversight community, researchers, industry, and the Congress to bring verifiable AI oversight to the cross-cutting work that GAO will continue to undertake.

Chairman Peters, Ranking Member Paul, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Taka Ariga at (202) 512-6888 or arigat@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Farahnaaz Khakoo-Mausel (Assistant Director), Jon D. Menaster (Analyst-in-Charge), Lisa Gardner, Nicole Catanzarite, Louise Fickel, Ryan Han, Lisa Gardner, Stephanie Palmer, and Evonne Tang.

Appendix I: Summaries of Key Practices in GAO's AI Accountability Framework

1. Governance

To help entities promote accountability and responsible use of AI systems, GAO identified key practices for establishing governance structures and processes to manage, operate, and oversee the implementation of these systems.

Key Practices

Governance at the Organizational Level

1.1 Clear goals: Define clear goals and objectives for the AI system to ensure intended outcomes are achieved.

1.2 Roles and responsibilities: Define clear roles, responsibilities, and delegation of authority for the AI system to ensure effective operations, timely corrections, and sustained oversight.

1.3 Values: Demonstrate a commitment to values and principles established by the entity to foster public trust in responsible use of the AI system.

1.4 Workforce: Recruit, develop, and retain personnel with multidisciplinary skills and experiences in design, development, deployment, assessment, and monitoring of AI systems.

1.5 Stakeholder involvement: Include diverse perspectives from a community of stakeholders throughout the AI life cycle to mitigate risks.

1.6 Risk management: Implement an AI-specific risk management plan to systematically identify, analyze, and mitigate risks.

Governance at the Systems Level

1.7 Specifications: Establish and document technical specifications to ensure the AI system meets its intended purpose.

1.8 Compliance: Ensure the AI system complies with relevant laws, regulations, standards, and guidance.

1.9 Transparency: Promote transparency by enabling external stakeholders to access information on the design, operation, and limitations of the AI system.


Example of an AI Governance Structure

In 2020, the Department of Defense (DOD) established an AI Executive Steering Group, which was created as the senior governance body to provide coordination and oversight of DOD's AI policies and activities. The Executive Steering Committee oversees nine subcommittees, one of which is on ethics. That subcommittee is responsible for providing practical guidance on how to apply the ethical principles for AI adopted by DOD to the different phases of the AI life cycle.

Selected Discussion from the Comptroller General Forum

- Entities should implement governance structures for AI systems that incorporate organizational values, consider risks, assign clear roles and responsibilities, and involve multidisciplinary stakeholders.
- Entities should define a governance structure that includes clear goals and objectives, which translates into systems requirements and performance metrics.
- Entities should include diverse perspectives from technical and non-technical communities throughout the AI life cycle to anticipate and mitigate unintended consequences including potential bias and discrimination.

Source: GAO. | GAO-23-106811
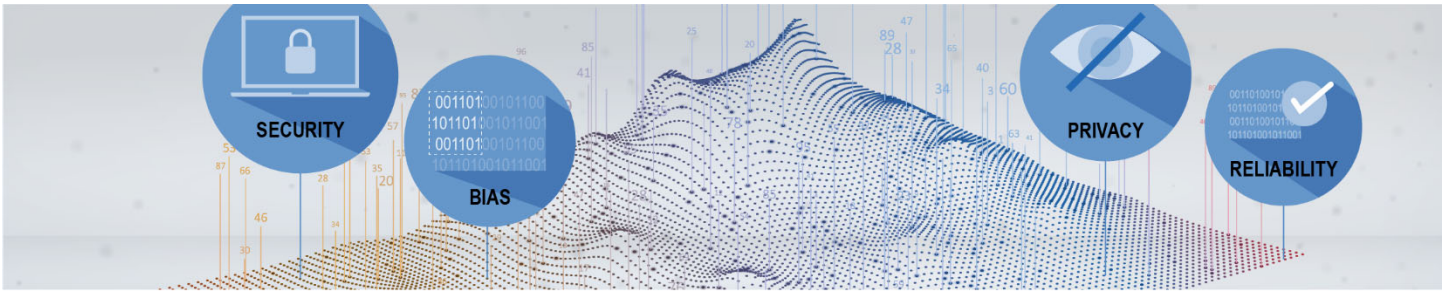
2. Data

To help entities use data that are appropriate for the intended use of each AI system, GAO identified key practices to ensure data are of high quality, reliable, and representative.

Key Practices

Data used for Model Development

2.1 Sources: Document sources and origins of data used to develop the models underpinning the AI system.

2.2 Reliability: Assess reliability of data used to develop the models**.**

2.3 Categorization: Assess attributes used to categorize data.

2.4 Variable selection: Assess data variables used in the AI component models.

2.5 Enhancement: Assess the use of synthetic, imputed, and/or augmented data.

Data Used for System Operation

2.6 Dependency: Assess interconnectivities and dependencies of data streams that operationalize the AI system.

2.7 Bias: Assess reliability, quality, and representativeness of all the data used in the system's operation, including any potential biases, inequities, and other societal concerns associated with the AI system's data.

2.8 Security and privacy: Assess data security and privacy for the AI system.

Example of Data Reliability

In 2019, the European Union Agency for Fundamental Rights released the report *Data Quality and Artificial Intelligence – Mitigating Bias and Error to Protect Fundamental Rights*. The report emphasizes the need for high-quality data and algorithms in machine learning systems and AI, and how transparency about data used in AI systems may help to prevent rights violations. The report also explains how AI systems use data, provides examples of how biases could be introduced, and provides examples of how low-quality data might affect accuracy and outcomes. Criteria for assessing data quality listed in the report include completeness, accuracy, consistency, timeliness, duplication, validity, availability, and whether the data are fit for the purpose.

Selected Discussion from the Comptroller General Forum

- Entities should provide documentation describing how training and testing data have been acquired or collected, prepared, and updated to demonstrate data quality and reliability.

- Entities should test data used in AI systems for biases. Biases may be introduced unintentionally during data collection and labeling.

- Entities should monitor data after deploying AI systems to identify potential data drift, which can lead to unintended consequences.

Source: GAO, majcot/stock.adobe.com (header); GAO (illustration). | GAO-23-106811
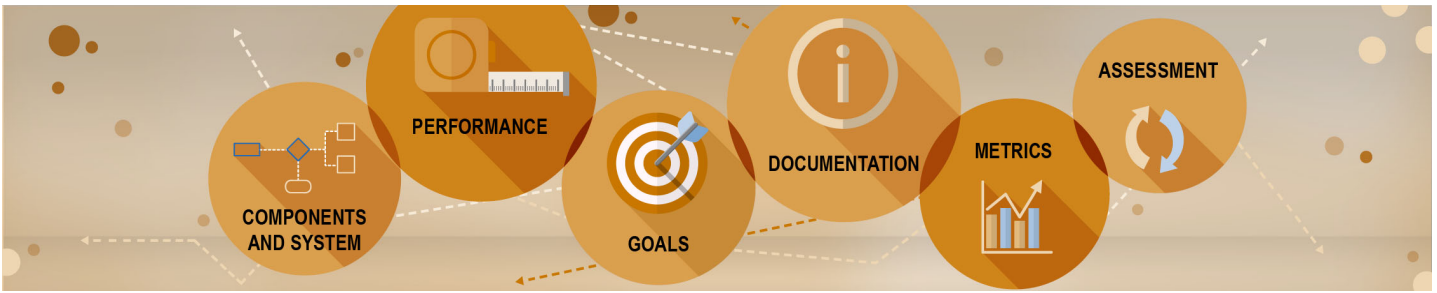
3. Performance

To help entities ensure AI systems produce results that are consistent with program objectives, GAO identified key practices for ensuring that systems meets their intended purposes.

Key Practices

Performance at the Component Level

3.1 Documentation: Catalog model and non-model components, along with operating specifications and parameters.

3.2 Metrics: Define performance metrics that are precise, consistent, and reproducible.

3.3 Assessment: Assess the performance of each component against defined metrics to ensure it functions as intended and is consistent with program goals and objectives.

3.4 Outputs: Assess whether outputs of each component are appropriate for the operational context of the AI system.

Performance at the System-Level

3.5 Documentation: Document the methods for assessment, performance metrics, and outcomes of the AI system to provide transparency over its performance.

3.6 Metrics: Define performance metrics that are precise, consistent, and reproducible.

3.7 Assessment: Assess performance against defined metrics to ensure the AI system functions as intended and is sufficiently robust.

3.8 Bias: Identify potential biases, inequities, and other societal concerns resulting from the AI system.

3.9 Human supervision: Define and develop procedures for human supervision of the AI system to ensure accountability.
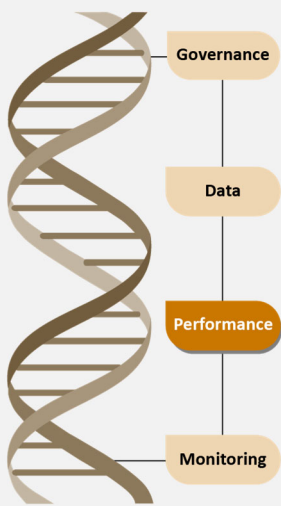
Example of Performance Documentation

Industry and nonprofit entities provided several examples of how entities can document performance by recording several aspects of AI systems, including intended use, specifications, testing methodology and test results, ethical considerations, and evaluation. Each of those examples includes questions or factors for consideration to guide entities in designing, developing, and deploying AI systems.

**Selected Discussion from the Comptroller General Forum**

- Entities should document requirements—including performance metrics—for the AI system throughout the life cycle.
- Entities should document methods to assess performance—which can include input-output tests, stress tests, and evaluations of model drift—to ensure AI systems meet their intended goals.
- Entities should provide access to performance test results, change logs, and other documentation describing updates and key design choices, and provide a copy of the model or algorithm code to third-party assessors of AI systems.
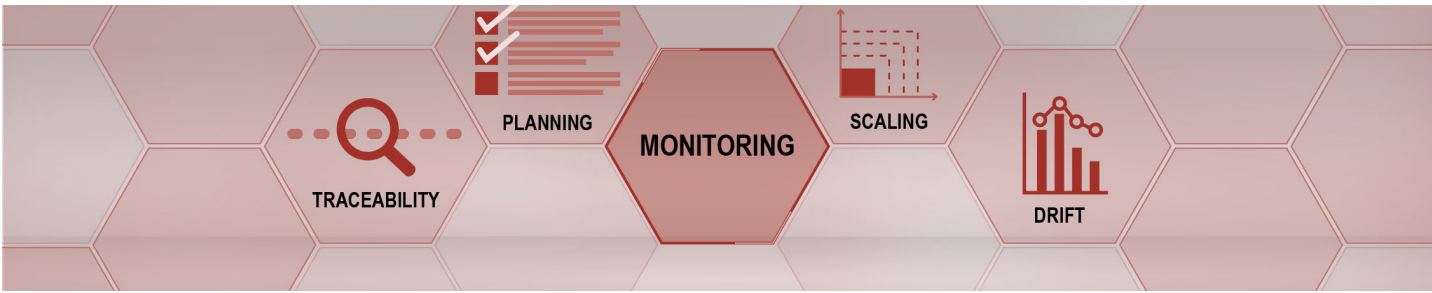
4. Monitoring

To help entities ensure reliability and relevance of AI systems over time, GAO identified key practices for monitoring performance and assessing sustainment and expanded use.
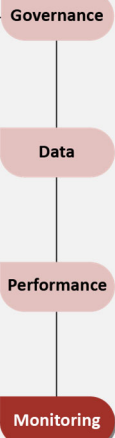
Key Practices

Continuous Monitoring of Performance

4.1 Planning: Develop plans for continuous or routine monitoring of the AI system to ensure it performs as intended.

4.2 Drift: Establish the range of data and model drift that is acceptable to ensure the AI system produces desired results.

4.3 Traceability: Document results of monitoring activities and any corrective actions taken to promote traceability and transparency.

Assessing Sustainment and Expanded Use

4.4 Ongoing assessment: Assess the utility of the AI system to ensure its relevance to the current context.

4.5 Scaling: Identify conditions, if any, under which the AI system may be scaled or expanded beyond its current use.

Example of Monitoring

In 2020, the World Economic Forum released the *Companion to the Model AI Governance Framework – Implementation and Self-Assessment Guide for Organizations*, which includes guidance on data monitoring and a discussion of ongoing monitoring, review, and tuning of AI algorithms and models. The guidance suggests updating AI systems based on changes in the operational environment, as well as documenting when and how the update took place, and the impact it had on the model outputs.

Selected Discussion from the Comptroller General Forum

- Entities should continuously monitor and evaluate the AI system to ensure it addresses program objectives.

- Entities should monitor changes in the data and models to ensure relevance and appropriateness.

- Entities should continuously monitor the AI system to ensure the system is appropriate in its current operating context.

Source: GAO. | GAO-23-106811

Appendix II: Selected List of GAO Reports on Artificial Intelligence

GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Machine Learning Technologies for Medical Diagnostics,* GAO-22-104629 (Washington, D.C.: Sept. 29, 2022).

GAO, *Facial Recognition Technology: Federal Agencies Use and Related Privacy Protections,* GAO-22-106100 (Washington, D.C.: June 29, 2022).

GAO, *Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance,* GAO-22-105834 (Washington, D.C.: Mar. 30, 2022).

GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems,* GAO-22-104765 (Washington, D.C.: Feb. 17, 2022).

GAO, *Digital Services: Considerations for a Federal Academy to Develop a Pipeline of Digital Staff,* GAO-22-105388 (Washington, D.C.: Nov. 19, 2021).

GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities,* GAO-21-519SP (Washington, D.C.: June 30, 2021).

GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO-21-518 (Washington, D.C.: June 3, 2021).

GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care,* GAO-21-7SP (Washington, D.C.: Nov. 30, 2020).

GAO, *Artificial Intelligence in Health Care: Benefits and Challenges of Machine Learning in Drug Development,* GAO-20-215SP (Washington, D.C.: Dec. 20, 2019, reissued Jan. 31, 2020).

GAO, *Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications,* GAO-18-142SP (Washington, D.C.: Mar. 28, 2018).