



Agency Use of Artificial Intelligence

Ad Hoc Committee on Agency Use of Artificial Intelligence

Draft Statement for Ad Hoc Committee | November 30, 2020

1 Artificial intelligence (AI) techniques are changing how government agencies do their
2 work.¹ Advances in AI hold out the promise of lowering the cost of completing government tasks
3 and improving the quality, consistency, and predictability of agency decisions. But enhanced
4 agency use of AI also raises concerns about the discretion being vested in AI systems and the
5 extent to which those systems are exercising authority that ought to be handled by human
6 officials.

7 Consistent with its statutory mission to promote efficiency, participation, and fairness in
8 administrative processes,² the Administrative Conference offers this Statement to identify issues
9 of which agencies should be mindful when adopting or modifying AI systems. The Statement
10 draws on a pair of reports commissioned by the Conference,³ as well as the input of AI experts
11 from government, academia, and the private sector.

¹ The National Institute of Standards and Technology has offered the following basic definition of AI:

AI technologies and systems are considered to comprise software [or] hardware that can learn to solve complex problems, make predictions or undertake tasks that require human-like sensing (such as vision, speech, and touch), perception, cognition, planning, learning, communications, or physical action. Examples are wide-ranging and expanding rapidly. They include, but are not limited to, AI assistants, computer vision systems, biomedical research, unmanned vehicle systems, advanced game-playing software, and facial recognition systems as well as application of AI in both Information Technology (IT) and Operational Technology (OT).

NAT'L INST. OF STANDARDS & TECH., U.S. LEADERSHIP IN AI: A PLAN FOR FEDERAL ENGAGEMENT IN DEVELOPING TECHNICAL STANDARDS AND RELATED TOOLS 7–8 (Aug. 9, 2019). The Administrative Conference adopts that definition for purposes of this statement.

² See 5 U.S.C. § 591.

³ DAVID FREEMAN ENGSTROM, DANIEL E. HO, CATHERINE M. SHARKEY, & MARIANO-FLORENTINO CUÉLLAR, GOVERNMENT BY ALGORITHM: ARTIFICIAL INTELLIGENCE IN FEDERAL ADMINISTRATIVE AGENCIES (2020),



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

12 The issues highlighted in this Statement are relevant to an array of agency personnel. To
13 minimize the risk of unforeseen problems involving an AI system, the agency should, throughout
14 the system’s lifespan, solicit input about the system from an array of offices—including, at a
15 minimum, the legal, policy, financial, human resources, and technology offices.

16 *1. Transparency*

17 Agencies’ efforts to ensure transparency in connection with their AI systems can serve
18 many valuable goals. When agencies set up processes to ensure transparency in their AI systems,
19 they should publicly identify the processes’ goals and the rationales behind them. For example,
20 an agency might prioritize transparency in the service of legitimizing its AI systems, facilitating
21 internal or external review of its AI-based decisionmaking, or coordinating its activities.
22 Different AI systems are likely to satisfy some transparency goals more than others. Where
23 possible, agencies should use metrics to measure the performance of their AI-transparency
24 processes.

25 In setting transparency goals, agencies should consider to whom they should be
26 transparent. For instance, depending on the nature of its operations, an agency might prioritize
27 transparency to the public, courts, Congress, or its own officials.

28 The appropriate level or nature of transparency and interpretability in an agency’s AI
29 systems will also depend on context. In some contexts, such as adjudication, reason-giving
30 requirements may call for a high degree of transparency and interpretability from the agency
31 regarding how an AI system functions. In other contexts, such as enforcement, an agency’s
32 legitimate interests in preventing gaming or adversarial learning by regulated parties could
33 militate against providing too much information (or specific types of information) to the public
34 about the AI system’s processes. In each context, agencies should consider whether particular
35 laws or policies governing disclosure of information apply.

<https://www.acus.gov/sites/default/files/documents/Government%20by%20Algorithm.pdf>; Cary Coglianese, *A Framework for Governmental Use of Machine Learning* (Oct. 2020), <https://www.acus.gov/sites/default/files/documents/Coglianese%20Report%20-%20A%20Framework%20for%20Governmental%20Use%20of%20Machine%20Learning.pdf> (draft report for Administrative Conference of the United States).



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

36 In selecting and using AI techniques, agencies should be cognizant of the degree to which
37 a particular AI system can be made transparent to appropriate people and entities, including the
38 general public. There may exist tradeoffs between explainability and accuracy in AI systems, so
39 that transparency and interpretability might sometimes weigh in favor of choosing simpler AI
40 models. The appropriate balance between explainability and accuracy will depend on the
41 agency's circumstances and priorities.

42 The proprietary nature of some AI systems may also affect the extent to which they can
43 be made transparent. When an agency's AI system relies on proprietary technologies or
44 algorithms the agency does not own, the agency and the public may have only limited access to
45 the information needed to understand the AI technique. Agencies should strive to anticipate such
46 circumstances and address them appropriately, such as by working with outside providers to
47 ensure they will be able to share sufficient information about such a system.

48 *2. Harmful Bias*

49 At their best, AI systems can help agencies identify and reduce the impact of unwanted
50 human biases.⁴ Yet they can also unintentionally create or exacerbate those biases by encoding
51 and deploying them at scale. In deciding whether and how to deploy an AI system, therefore,
52 agencies should carefully evaluate the biases that might result from the use of the AI system as
53 well as the biases that might result from alternative systems that rely on human actors (such as an
54 incumbent system that the AI system would augment or replace). Because different types of bias
55 pose different types of harms, the outcome of the evaluation will depend on the agency's unique
56 circumstances and priorities and the consequences posed by those harms in that context.

57 AI systems can be biased because of their reliance on data reflecting historical human
58 biases or because of their designs. Biases in AI systems can increase over time through feedback,
59 which can occur if the use of a biased AI system leads to systematic errors in categorizations,

⁴ The term *bias* has a technical meaning in the machine learning literature related to model characteristics. Under some circumstances, increasing bias (roughly the error of the average prediction) can improve system performance, if it reduces the risk of overfitting. Here, the Administrative Conference uses the term more generally to refer to common or systematic errors in decision making, especially those implicating normative concerns related to fairness and equal treatment.



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

60 which are then reflected in the data set or data environment the system uses to make future
61 predictions. Agencies should be mindful of the interdependence of the models, metrics, and data
62 that underpin AI systems.

63 Identifying biases in AI systems can pose challenges, as when the bias affects a particular
64 population but information about which individuals are in that population is not directly
65 available. To identify and mitigate such biases, agencies should, to the extent practical, consider
66 whether other data or methods are available.

67 Data science techniques for identifying and mitigating biases in AI systems are
68 developing. Agencies should stay up to date on developments in the field of AI, particularly on
69 algorithmic fairness; establish processes to ensure that people with diverse perspectives are able
70 to inspect AI systems and their decisions for indications of harmful bias; test AI systems in
71 environments resembling the ones in which they will be used; and make use of internal and
72 external processes for evaluating the risks of bias in AI systems.

73 *3. Technical Capacity*

74 AI systems can help agencies conserve resources, but they can also require substantial
75 investments of human and financial capital. Agencies should carefully evaluate the short- and
76 long-term costs and benefits of an AI system before committing significant resources to it. Each
77 agency should also ensure it has access to the technical expertise required to make informed
78 decisions about the type of AI systems it requires, how to integrate those systems into its
79 operations, and how to oversee, maintain, and update those systems.

80 Given the data science field's ongoing and rapid development, agencies should consider
81 cultivating an AI-ready workforce, including through recruitment and training efforts that
82 emphasize AI skills. When agency personnel lack the skills to develop, procure, or maintain an
83 AI system that meets the agency's needs, the agency should consider other means of expanding
84 its technical expertise, including by relying on tools such as the Intergovernmental Personnel



85 Act,⁵ prize competitions, or cooperative research and development agreements with private
86 institutions or universities.

87 *4. Obtaining AI Systems*

88 Decisions about whether or how to obtain an AI system can involve important trade-offs.
89 Buying an AI system from an external source might allow the agency to acquire a more
90 sophisticated tool than it could design on its own, access that tool sooner, and save some of the
91 up-front costs associated with developing the technical capacity needed to design an AI system.
92 Creating an AI tool within the agency, by contrast, might yield a tool that is better tailored to the
93 agency's particular tasks and policy goals. Creating an AI system within the agency can also
94 facilitate development of internal technical capability, which can yield benefits over the lifetime
95 of the AI system and in other technological tasks the agency may confront.

96 Certain government offices are available to help agencies with decisions and actions
97 related to technology.⁶ Agencies should make appropriate use of these resources when obtaining
98 an AI system.

99 *5. Data*

100 AI systems require data, often in vast quantities. An agency should consider whether it
101 has, or can obtain, data that appropriately reflects conditions similar to the ones the agency's AI
102 systems will address in practice; whether the agency has the resources to render the data into a
103 format that can be used by the agency's AI systems; and how the agency will maintain the data
104 and link it to the agency's AI systems without compromising security or privacy.

105 *6. Privacy*

⁵ 5 U.S.C. §§ 3371–76.

⁶ Within the General Services Administration, for example, the office called 18F routinely partners with government agencies to help them build and buy technologies. Similarly, the United States Digital Service has a staff of technologists whose job is to help agencies build better technological tools. While the two entities have different approaches—18F acts more like an information intermediary and the Digital Service serves as an alternative source for information technology contracts—both could aid agencies with obtaining, developing, and using different AI techniques.



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

106 Agencies have a responsibility to protect privacy with respect to personally identifiable
107 information in AI systems no less than in other aspects of agency operation. In a narrow sense,
108 this responsibility demands that agencies comply with requirements related to transparency, due
109 process, accountability, and information quality and integrity established by the Privacy Act of
110 1974, Section 208 of the E-Government Act of 2002, and other laws and policies.⁷ More broadly,
111 agencies should recognize and appropriately manage privacy risks posed by an AI system.
112 Agencies should consider privacy risks throughout the entire development life cycle of an AI
113 system and assess those risks, as well as associated controls, on an ongoing basis. The Office of
114 Management and Budget and the National Institute of Standards and Technology have developed
115 risk management frameworks that agencies may find useful in implementing AI systems.⁸

116 *7. Security*

117 Agencies should consider the possibility that AI systems might be manipulated, fooled,
118 evaded, and misled, including through manipulation of training data and exploitation of model
119 sensitivities. An agency must ensure not only that its data is secure, but also that its AI systems
120 are trained on that data in a secure manner, make forecasts based on that data in a secure manner,
121 and otherwise operate in a secure manner. Agencies should continuously consider and evaluate
122 the safety and security of AI systems, including resilience to vulnerabilities, manipulation, and
123 other malicious exploitation. The Risk Management Framework is also a tool for agencies to
124 utilize in addressing information security risks.⁹

125 *8. Decisional Authority*

126 Agencies should be mindful that most AI systems will involve human beings in a range
127 of capacities—as operators, customers, overseers, policymakers, or interested members of the

⁷ See, e.g. 5 U.S.C. § 552a(e), (g), & (p); 44 U.S.C. § 3501 note.

⁸ See, e.g., Nat'l Inst. of Standards & Tech., *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (Jan. 16, 2020); Nat'l Inst. of Standards & Tech. Special Publication SP-800-37 revision 2, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy* (Dec. 2018); Office of Mgmt. & Budget, Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

⁹ See *id.*



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

128 public. Accordingly, any decision to deploy an AI system should account for the human
129 tendencies and preferences of humans in those roles.

130 Human factors may sometimes undercut the value of using AI systems to make certain
131 determinations. There is a risk, for example, that human operators will devolve too much
132 responsibility to AI systems and fail to detect cases where the AI systems yield inaccurate or
133 unreliable determinations. That risk may be tolerable in some settings—such as when the AI
134 system has recently been shown to perform significantly better than alternatives—but intolerable
135 in others.

136 Similarly, if agency personnel come to rely reflexively on algorithmic results in
137 exercising discretionary powers, use of an AI system could have the practical effect of curbing
138 the exercise of agency discretion or shifting it from the person who is supposed to be exercising
139 it to the system’s designer. Agencies should beware of such potential shifts of practical authority
140 and take steps to ensure that appropriate officials have the knowledge and power to be
141 accountable for decisions made or aided by AI techniques.

142 Finally, there may be some circumstances where, for reasons wholly apart from
143 decisional accuracy, an agency may wish to have a decision be made by a human being, even if
144 the law does not require it. In some contexts, accuracy and fairness are not the only relevant
145 values at stake, and an AI system may be difficult to sustain if human beings perceive it as
146 unfair, inhumane, or otherwise unsatisfactory.¹⁰

147 9. Oversight

148 It is essential that agencies’ AI systems be subject to appropriate and regular oversight
149 throughout their lifespans. There are two general categories of oversight: external and internal.
150 An agency’s mechanisms of internal oversight will be shaped by the demands of external

¹⁰ Cf. Admin. Conf. of the U.S., Recommendation 2018-3, *Electronic Case Management in Federal Administrative Adjudication*, 83 Fed. Reg. 30,686 (June 29, 2018) (suggesting, in the context of case management systems, that agencies consider implementing electronic systems only when they conclude that doing so would lead to benefits without impairing either the objective “fairness” of the proceedings or the subjective “satisfaction” of those participating in those proceedings).



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

151 oversight. And the more effective an agency’s internal oversight mechanisms, the better it is
152 likely to fare with external oversight. An agency should be cognizant of both forms of oversight
153 in making decisions about its AI systems.

154 External oversight of agency use of AI systems can come from a variety of government
155 sources, including inspectors general, the Government Accountability Office, and Congress.
156 Courts can also play an important role in external oversight of agency uses of AI systems.
157 Agency uses of AI systems might lead to litigation in a number of circumstances. Those affected
158 by an agency’s use of an AI system might, for example, allege that use of the system violates
159 their right to procedural due process.¹¹ Or they might allege that the AI system’s determination
160 violated the Administrative Procedure Act (APA) because it was arbitrary and capricious.¹²
161 When an AI system narrows the discretion of agency personnel, or fixes or alters the legal rights
162 and obligations of people subject to the agency’s action, affected people or entities might also
163 sue on the ground that the AI system is a legislative rule adopted in violation of the APA’s
164 requirement that legislative rules go through the notice-and-comment process.¹³ Agencies should
165 consider these different forms of potential external oversight as they are making and
166 documenting decisions about AI systems and as they are developing processes for making those
167 decisions.

168 Agencies should also develop their own, internal evaluation and oversight mechanisms
169 for their uses of AI systems, taking into account their system-level risk management,
170 authorization to operate, and continuous monitoring responsibilities, and their broader enterprise
171 risk management responsibilities.¹⁴ Successful internal oversight requires advance and ongoing
172 planning and consultation with the various offices in an agency that will be affected by the

¹¹ Courts would analyze such challenges under the three-part balancing framework from *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976).

¹² See 5 U.S.C. § 706(2)(A). Courts would review such challenges under the standard set forth in *Motor Vehicle Manufacturers Ass’n v. State Farm Mutual Automobile Insurance Co.*, 463 U.S. 29, 43 (1983).

¹³ See 5 U.S.C. § 553(b)–(c).

¹⁴ See Office of Mgmt. & Budget, Circular A-130, *supra* n.8; Office of Mgmt. & Budget, Circular A-123, *Management’s Responsibilities for Enterprise Risk Management and Internal Control* (July 15, 2016)



ADMINISTRATIVE CONFERENCE OF THE UNITED STATES

173 agency's use of an AI system, including its legal, policy, financial, human resources, and
174 technology offices. An agency's oversight plan should address how the agency will pay for its
175 oversight mechanisms and how it will respond to what it learns from its oversight.

176 Agencies should establish a protocol for regularly evaluating AI systems throughout the
177 systems' lifespans. That is particularly true if a system or the circumstances in which it is
178 deployed are liable to change over time, since, in that case, review and explanation of the
179 system's functioning at one stage of development or use may become outdated due to changes in
180 the system's underlying models. To enable that type of oversight, agencies should monitor and
181 keep track of the data being used by their AI systems, as well as how the systems use that data.
182 Agencies may also wish to secure input from members of the public or private evaluators to
183 improve the likelihood that they will identify defects in their AI systems.

184 To make their oversight systems more effective, agencies should clearly define goals for
185 their AI systems. The relevant question for oversight purposes will often be whether the AI
186 system outperforms alternatives, which may require the agency to benchmark the system against
187 the status quo or some hypothetical state of affairs.

188 Finally, AI systems can affect how agency staff do their jobs, particularly as agency
189 personnel grow to trust and rely on the systems. In addition to evaluating and overseeing their AI
190 systems, agencies should pay close attention to how agency personnel interact with those
191 systems.