epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

FEEDBACK OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

National Institute of Standards and Technology

Regarding the

Artificial Intelligence Risk Management Framework

August 18th, 2021

The Electronic Privacy Information Center ("EPIC") submits the following feedback to the request for information by the National Institute of Standards and Technology ("NIST") on the AI Risk Management Framework (hereinafter, the "AI RMF").[1]

EPIC is a public interest research center in Washington, D.C. that was established in 1994 to focus public attention on emerging privacy and related human rights issues and to protect privacy, the First Amendment, and constitutional values.[2] EPIC has a long history of promoting transparency and accountability for information technology.[3]

EPIC has a particular interest in promoting algorithmic transparency and has consistently advocated for the adoption of the Universal Guidelines for AI ("UGAI") to promote trustworthy algorithms and justice for individuals harmed by certain AI systems.[4] EPIC has advocated for

---

[1] Artificial Intelligence Risk Management Framework, National Institute of Standards and Technology (August 2021), https://www.federalregister.gov/documents/2021/07/29/2021-16176/artificial-intelligence-risk-management-framework.

[2] EPIC, *About EPIC* (2019), https://epic.org/epic/about.html.

[3] EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/; Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6, https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf.

[4] *See* e.g. EPIC v. DOJ (D.C. Cir.) (18-5307), https://epic.org/foia/doj/criminal-justice-algorithms/; Comments of EPIC, *Intellectual Property Protection for Artificial Intelligence Innovation*, U.S. Patent and Trademark Office (Jan. 10, 2020), https://epic.org/apa/comments/EPIC-USPTO-Jan2020.pdf; Comments of EPIC, *HUD's Implementation of the Fair Housing Act's Disparate Impact Standard*, Department of Housing and Urban Development (Oct. 18, 2019), https://epic.org/apa/comments/EPIC-HUD-Oct2019.pdf; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019),

transparency and accountability internationally related to the use of AI systems, litigating cases against the U.S. Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[5] and against the U.S. Department of Homeland Security to produce documents about a program purported to assess the probability of whether an individual committed a crime.[6] In 2018, EPIC and leading scientific societies petitioned the U.S. Office of Science and Technology Policy to solicit public input on U.S. Artificial Intelligence Policy.[7] EPIC submitted comments urging the National Science Foundation to adopt the UGAI and to promote and enforce the UGAI across funding, research, and deployment of U.S. AI systems.[8] EPIC has also recently submitted comments to the National Security Commission on Artificial Intelligence, the U.S. Office of Science and Technology Policy, the European Commission, and the U.S. Office of Management and Budget urging the adoption of AI system regulation that meaningfully protects individuals.[9]

In an effort to establish necessary consumer safeguards, EPIC filed FTC complaints against HireVue,[10] a company that sells algorithmic employment screening, and AirBnB,[11] the rental service that claims to assess risk in potential renters based on an opaque algorithm. EPIC has also filed a petition with the FTC for a rulemaking for AI in Commerce.[12] EPIC also published the *AI Policy Sourcebook*, the first reference book on AI policy.[13]

---

https://epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; Statement of EPIC, *Industries of the Future*, U.S. Senate Committee on Commerce, Science & Transportation (Jan. 15, 2020), https://epic.org/testimony/congress/EPIC-SCOM-AI-Jan2020.pdf; Comments of EPIC, *Request for Information: Big Data and the Future of Privacy*, Office of Science and Technology Policy (Apr. 4, 2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf.

[5] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)*, https://epic.org/foia/doj/criminal-justice-algorithms/.

[6] *See Id.* and EPIC, *EPIC v. DHS (FAST Program),* https://epic.org/foia/dhs/fast/.

[7] EPIC, Petition to OSTP for Request for Information on Artificial Intelligence Policy (July 4, 2018), https://epic.org/privacy/ai/OSTP-AI-Petition.pdf.

[8] EPIC, Request for Information on Update to the 2016 National Artificial Intelligence Research and Development Strategic Plan, National Science Foundation, 83 FR 48655 (Oct. 26, 2018), https://epic.org/apa/comments/EPIC-Comments-NSF-AI-Strategic-Plan-2018.pdf.

[9] Comments of EPIC, *Solicitation of Written Comments by the National Security Commission on Artificial Intelligence*, 85 Fed. Reg. 32,055, National Security Commission on Artificial Intelligence (Sep. 30, 2020), https://epic.org/apa/comments/EPIC-comments-to-NSCAI-093020.pdf; Comments of EPIC, *Request for Comments on a Draft Memorandum to the Heads of Executive Departments and Agencies, "Guidance for Regulation of Artificial Intelligence Applications,"* 85 Fed. Reg. 1825, Office of Management and Budget (Mar. 13, 2020), https://epic.org/apa/comments/EPIC-OMB-AI-MAR2020.pdf; Comments of EPIC, *Request for Feedback in Parallel with the White Paper on Fundamental Rights*, European Commission Fundamental Rights Policy Unit (May 29, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Comments-May2020.pdf; Comments of EPIC, *Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence*, European Commission (Sep. 10, 2020), https://epic.org/apa/comments/EPIC-EU-Commission-AI-Sep2020.pdf.

[10] Complaint and Request for Investigation, Injunction, and Other Relief, *In re HireVue* (Nov. 6, 2019), https://epic.org/privacy/ftc/hirevue/EPIC_FTC_HireVue_Complaint.pdf.

[11] Complaint and Request for Investigation, Injunction, and Other Relief, *In re Airbnb* (Feb. 27, 2019), https://epic.org/privacy/ftc/airbnb/EPIC_FTC_Airbnb_Complaint_Feb2020.pdf.

[12] *In re: Petition for Rulemaking Concerning Use of Artificial Intelligence in Commerce*, EPIC (Feb. 3, 2020), https://epic.org/privacy/ftc/ai/EPIC-FTC-AI-Petition.pdf.

[13] *EPIC AI Policy Sourcebook 2020* (EPIC 2020), https://epic.org/bookstore/ai2020/.

EPIC applauds the efforts NIST has made to substantively incorporate public input and transparency in the AI RMF development process and we encourage NIST to continue these efforts. In crafting the AI RMF, EPIC recommends that NIST (i) draft the AI RMF with an eye toward interoperability with current and forthcoming AI system regulations, guidance, and standards; (ii) prioritize the protection of individuals impacted by AI systems; and (iii) build in a strong standard of accountability and enforcement for both public and private entities using AI. EPIC has provided specific feedback below for certain questions posed by NIST relating to AI RMF development.

EPIC Recommends NIST Recognize and Address Current and Potential Algorithmic Harm to Individuals, Build in Meaningful and Substantive Accountability and Enforcement Measures, and Draw From and Bolster Rights-Protecting Frameworks in the AI RMF Draft

NIST Information Request 1: The greatest challenges in improving how AI actors manage AI-related risks—where "manage" means identify, assess, prioritize, respond to, or communicate those risks.

There are multiple challenges to managing AI-related risk, but before addressing any management proposals, it is imperative that we recognize the scope of AI-related risk. One of the clearest risks stemming from AI is negative impact that use of these systems may have on individuals whose information is processed within them—in particular where that impact is tied to bias or discrimination.[14] Decisions made by AI systems may impact individuals in matters of housing, credit, education, employment, and criminal justice, making it imperative that AI systems are regularly assessed to ensure (i) that they are accurate, do not lead to disparate impacts on the basis of a protected class, or cause privacy harms; (ii) that meaningful evaluations of potential risk versus perceived benefit take place; and (iii) that harmful systems and systems that violate regulations and standards are subject to enforcement measures. Finally, the guidelines, regulations, and standards for AI systems must be clear and consistent, empowering individuals to know their rights and requiring companies using AI systems to be aware of their obligations.

First, the AI RMF must contain substantive protections for individuals affected by AI systems (that is, any individual whose personal data is entered into or processed through an AI system). The exact form of protection may vary, but likely would include data subject rights, mandatory notice to affected individuals (prior to processing where possible), consent mandates where applicable, security measures, and requirements specifically barring any AI systems or uses that further perpetuate discrimination or bias. In addition, sensitive characteristics should have

[14] *See e.g.* Complaint for Permanent Injunction and Other Equitable Relief at 34-35, F.T.C. v. CompuCredit Corp., No. 1:08–CV–1976–BBM–RGV (N.D. Ga. Oct. 8, 2008), https://www.ftc.gov/sites/default/files/documents/cases/2008/06/080610compucreditcmptsigned.pdf (In which the FTC brought suit against a credit card company that allegedly used an undisclosed behavioral scoring algorithm to determine credit limitations based on consumer conduct); James Vincent, The Invention of AI 'Gaydar' Could be the Start of Something Much Worse, The Verge (Sept. 21, 2017), https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy; Claudia Garcia-Rojas, The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies, Truthout (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police (Discussing Professor Simone Brown's research on how race and anti-Black colonial logics inform contemporary surveillance practices).

specific protections—sensitive characteristics would include, for example, the information of children or information specifically pertaining to race, sexuality, gender, or ethnicity.[15]

EPIC also recommends that emotion recognition systems and biometric categorization systems be banned outright. Emotion recognition systems rely on algorithms based on the idea that both universal emotions and a clear correlation between emotion and facial expression exist—beliefs that have since been disproven.[16] Similarly, biometric categorization systems are based on the belief that certain physical characteristics can be linked to specific traits. This is essentially a form of digital phrenology.[17] Companies using these system types have claimed to be able to predict anything from the likelihood of terrorist leanings to sexuality based solely on analyzing facial features.[18] Both of these system types have persistent and inherent problems of both inaccuracy and bias that cannot be divided from the systems or meaningfully resolved such that they do not cause harm. EPIC believes these systems to be harmful by their very nature and urges NIST to ban them entirely.

Next, there must be real accountability measures and enforcement for non-compliance included within the AI RMF. Without oversight, measurable demonstrations of compliance efforts, and the possibility of enforcement actions where users of AI systems do not meet the requirements of the AI RMF, there is minimal incentive for companies to prioritize or allocate resources for compliance. The AI RMF may be able to draw from accountability features present in other proposed and active regulations, guidelines, and frameworks, such as fines and injunctions for violations, mandatory impact assessments prior to deployment of an AI system, third party audits of systems—particularly where a system may be considered high-risk, internal checklists and reports

---

[15] See e.g., Claudia Garcia-Rojas, *supra* note 14; James Vincent, *supra* note 14.

[16] Kate Crawford, Artificial Intelligence is Misreading Human Emotion, The Atlantic (Apr. 27, 2021), https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/; Lisa Feldman Barret et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements, 20 Ass'n for Psych. Sci., 1, 46 (2019), available at https://journals.sagepub.com/doi/pdf/10.1177/1529100619832930; see also Krys, Kuba et al., Be Careful Where You Smile: Culture Shapes Judgments of Intelligence and Honesty of Smiling Individuals, Journal of Nonverbal Behavior Vol. 40, 101-116 (2016), available at https://doi:10.1007/s10919-015-0226-4; Charlotte Gifford, The Problem with Emotion-Detection Technology, The New Economy (June 15, 2020), https://www.theneweconomy.com/technology/the-problem-with-emotion-detection-technology.

[17] Blaise Aguera y Arcas et al., Physiognomy's New Clothes, Medium (May 6, 2017), https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a.

[18] See Sally Adee, Controversial Software Claims to Tell Your Personality From Your Face, New Scientist (May 27, 2016), https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/; Researchers are Using Machine Learning to Screen for Autism in Children, Duke Pratt School of Engineering (July 11, 2019), https://pratt.duke.edu/about/news/amazon-autism-app-video; Paul Lewis, "I was Shocked it was so Easy": Meet the Professor Who Says Facial Recognition Can Tell if You're Gay, The Guardian (July 7, 2018), https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis; Madhi Hashemi & Margaret Hall, Criminal Tendency Detection from Facial Images and the Gender Bias Effect, 7 J. Big Data, 1, 1 (2020), https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0282-4#Sec9 (since retracted); Luana Pascu, Biometric Software that Allegedly Predicts Criminals Based on Their Face Sparks Industry Controversy, Biometric Update (May 6, 2020), https://www.biometricupdate.com/202005/biometric-software-that-allegedly-predicts-criminals-based-on-their-face-sparks-industry-controversy.

documenting meaningful engagement with the AI RMF requirements, and transparency with authorities and affected individuals. An additional enforcement approach that would align with currently-proposed privacy legislation is disgorgement.[19] The current draft of the Data Protection Act of 2021 includes measures for disgorgement of any revenue, data, or technology acquired through violation of a regulation or rule or order of an oversight agency.[20] NIST may want to consider this, both as a way to dissuade improper use of AI systems and to coordinate with pending legislation.

Finally, there are currently few obligations, requirements, or uniformly-applicable standards for entities developing or using AI. However, this is swiftly changing. Multiple regulations, frameworks, and guidelines have been proposed in the past year directly aimed at AI systems.[21] In drafting the AI RMF, NIST should evaluate the specific requirements, obligations, and stipulations contained in these measures and ensure that the AI RMF does not contradict these regulations or enshrine a lower standard of protection that would weaken these measures or cause confusion, either for AI system operators or individuals affected by AI systems.

NIST Information Request 7: AI risk management standards, frameworks, models, methodologies, tools, guidelines and best practices, principles, and practices which NIST should consider to ensure that the AI RMF aligns with and supports other efforts.

There have been several AI principles proposed by industry, academia, civil society, and governments. Of these, EPIC recommends that NIST use principles from the UGAI and the OECD AI Principles to guide the AI RMF.

The UGAI framework for AI governance, based on the protection of human rights, was presented at the 2018 Public Voice meeting in Brussels, Belgium.[22] The UGAI has been endorsed by more than 250 experts and 60 organizations in 40 countries.[23] Widespread endorsement of the UGAI principles indicates that adoption of the principles would help to align the AI RMF with predominant global standards. We recommend that the elements of the UGAI be incorporated where possible when developing the AI RMF and that NIST should ensure that the AI RMF is compatible with the UGAI. The UGAI comprises twelve principles:

1. Right to Transparency
2. Right to Human Determination
3. Identification Obligation
4. Fairness Obligation

---

[19] S. 2134, 117th Cong. (2021).
[20] *Id.* at §13(e)(1)(B)(4).
[21] *See Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021); Public consultation on the OECD Framework for Classifying AI Systems, Organisation for Economic Cooperation and Development (June 2021) https://oecd.ai/classification; Recommendation of the Council on Artificial Intelligence, OECD (May 21, 2019) [hereinafter OECD AI Principles], https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[22] *Universal Guidelines for Artificial Intelligence*, The Public Voice (Oct. 23, 2018) [hereinafter *Universal Guidelines*], https://thepublicvoice.org/ai-universal-guidelines/.
[23] *Id.*

5. Assessment and Accountability Obligation
6. Accuracy, Reliability, and Validity Obligations
7. Data Quality Obligation
8. Public Safety Obligation
9. Cybersecurity Obligation
10. Prohibition on Secret Profiling
11. Prohibition on Unitary Scoring
12. Termination Obligation[24]

NIST should also review and consider incorporating the AI principles adopted by the Organization of Economic Cooperation and Development ("OECD AI Principles").[25] The OECD AI Principles were adopted in 2019 and endorsed by 42 countries—including several European Countries, the United States, and the G20 nations.[26] While largely aligning with the principles of the UGAI, the OECD AI Principles provide additional considerations that may be beneficial to development of the AI RMF. Adopting the OECD AI Principles would not only assist with interoperability but would also address the additional identified key principles of meaningful protections for individuals and accountability. The OECD AI Principles establish international standards for AI use:

1. Inclusive growth, sustainable development and well-being
2. Human-centered values and fairness
3. Transparency and explainability
4. Robustness, security, and safety
5. Accountability[27]

NIST should also be guided by Office of Management and Budget ("OMB") draft guidance regarding how federal agencies should regulate AI. The draft OMB guidance published on January 7, 2020, called on agencies, when considering regulations or policies related to AI applications, "to promote advancements in technology and innovation, while protecting American technology, economic and national security, privacy, civil liberties, and other American values."[28] The principles set forth in the draft regulation are:

1. Public Trust[29]
2. Public Participation[30]
3. Scientific Integrity and Information Quality[31]

---

[24] *Id.*
[25] *Recommendation of the Council on Artificial Intelligence*, OECD (May 21, 2019) [hereinafter *OECD AI Principles*], https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[26] *U.S. Joins with OECD in Adopting Global AI Principles*, NTIA (May 22, 2019), https://www.ntia.doc.gov/blog/2019/us-joins-oecd-adopting-global-ai-principles.
[27] *OECD AI Principles*, *supra* note 25.
[28] *Draft Memorandum for the Heads of Executive Departments and Agencies*, Office of Management and Budget, January 7, 2020 https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.
[29] OMB Guideline 1.
[30] OMB Guideline 2.
[31] OMB Guideline 3.

4. Risk Assessment and Management[32]
5. Benefits and Cost[33]
6. Flexibility[34]
7. Fairness and Non-discrimination[35]
8. Disclosure and Transparency[36]
9. Safety and Security[37]
10. Interagency Coordination[38]

NIST Information Request 9: The appropriateness of the attributes NIST has developed for the AI Risk Management Framework.

NIST identified several relevant attributes that they believe should be considered throughout the AI RMF development process: (i) be consensus driven and regularly updated through an open and transparent process; (ii) provide common definitions; (iii) use plain and understandable language; (iv) be risk-based, outcome-focused, voluntary, and non-prescriptive; (v) fit into an entity's broader risk management strategy; and (vi) be a living document capable of being updated with developments in technology and culture.[39]

Broadly, these are appropriate attributes and EPIC applauds NIST's commitment to an open and transparent process. EPIC encourages NIST to continue engaging with a diverse set of experts and the public at large while developing the AI RMF. While the AI RMF is aimed mostly at designing, developing, and using AI, EPIC urges NIST to consider perspectives from both those evaluating AI and those affected by AI in creating this tool, as well as privacy advocates and experts with knowledge of how this technology will be developed and deployed. Ultimately, the AI RMF should yield a readable result that helps individuals understand the systems being used.

EPIC recommends strengthening these attributes and adding additional goals that protect human rights. Specifically, NIST should consider making the framework mandatory for certain sensitive applications. In addition, as an expert body that can play a key role in the development of AI regulation, NIST should develop an AI RMF that can inform policy development and updates from federal and state regulators. The AI RMF has the potential to empower individuals who are the subjects of AI systems to understand more about the risk of these systems and more successfully navigate their own involvement, as well as identifying the entities in power contracting, buying, or implementing these systems.

[32] OMB Guideline 4.
[33] OMB Guideline 5.
[34] OMB Guideline 6.
[35] OMB Guideline 7.
[36] OMB Guideline 8.
[37] OMB Guideline 9.
[38] OMB Guideline 10.
[39] Artificial Intelligence Risk Management Framework, supra note 1 at 40811-40812.

NIST Information Request 12: The extent to which the Framework should include governance issues, including but not limited to make up of design and development teams, monitoring and evaluation, and grievance and redress.

The AI RMF must incorporate meaningful measures of accountability in order to ensure that AI systems meet legal and ethical requirements and to incentivize compliance for companies engaged in algorithmic practices. The use of impact assessments, ongoing review and evaluation of AI systems, and substantial enforcement for violations of these requirements should be considered as useful and measurable ways to mandate accountability within the AI RMF draft.

There are currently nearly no regulatory reporting requirements—either prior to or during deployment—for the vast majority of AI tools in the U.S. The AI RMF can serve to remedy this gap. In some countries, such as Canada, certain AI systems used in public contexts must undergo Algorithmic Impact Assessments that assess the riskiness of an individual system based on the sensitivity of data, certain design attributes, and relation to areas designated as requiring additional considerations and protections.[40] A few examples of questions in the Canadian tool include prompts to evaluate the stakes of decisions the system in question makes, vulnerability of subjects, and whether it is a predictive risk assessment.[41] The tool also allows for multiple answer options and detailed explanation of responses. Certain aspects of the Canadian assessment require identification of the downstream processes of a system. This identification process includes asking (i) will the system only be used to assist a decision-maker; (ii) will the system be replacing a decision that would otherwise be made by a human; (iii) will the system be replacing human judgment; (iv) whether the system is being used by the same entity that developed it; and (v) consideration and explanation about both economic and environmental impacts.[42] NIST should consider requiring similar elements in any assessments for AI systems under the AI RMF.

Another potential approach to accountability can be found in the European Commission's proposed regulatory system that would modify governance requirements, restrictions, and levels of AI system evaluation according to the risk level of that AI system and its proposed use. In evaluations under the European Commission's Proposed Artificial Intelligence Act, there are tiers of risky AI applications, including unacceptable AI and high-risk AI, which trigger different regulatory action.[43] This tiered approach to adapting governance requirements to the level of risk could be a useful approach for the AI RMF, imposing more advanced requirements on companies using high-risk systems and ensuring that individual protections remain strong for high-risk endeavors.

With the exception of local ordinances about specific topics and proposed state laws, similar impact assessment requirements or significant disclosure requirements do not exist in U.S. law, though such requirements are included in legislative proposals.[44] This current lack of review and evaluation of systems provides an opportunity for NIST's development of the AI RMF to help guide

[40] Canada Digital Services, Algorithmic Impact Assessment (last visited June 9, 2021), available at https://open.canada.ca/aia-eia-js/?lang=en.
[41] *Id*.
[42] *Id*.
[43] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).
[44] *See e.g.* S. 2134, 117th Cong. (2021), H.R. 2231, 116th Cong. (2019).

and shape the U.S. approach to regulating AI system development and deployment. At minimum, NIST should mandate that compliance with AI RMF standards will be required for entities using AI systems in ways that process sensitive information or will be used in sensitive contexts, such as criminal justice, education, credit scoring, housing, and hiring.

The AI RMF can interact with governance, makeup of teams, and offering of grievance and redress by encouraging direct consideration of these factors, possibly through requiring developers and purchasers to complete reports or internal checklists considering these areas. Although it would be preferable for requirements of governance, grievance, and redress to come from the legislature to have broad applicability and protective power, NIST may be able to shape the common practices through its AI RMF draft which will in turn influence any legislation that may develop at a later time.

Conclusion

EPIC recommends that NIST prioritize the following when developing the AI RMF: the protection of individuals impacted by AI systems, interoperability and compatibility with current regulation and standards related to AI, and meaningful accountability and enforcement measures.

Respectfully Submitted,

/s/ *Calli Schroeder*
Calli Schroeder
EPIC Global Privacy Counsel

/s/*Ben Winters*
Ben Winters
EPIC Equal Justice Works Fellow