RECOMMENDATION: Require Public Summary Reporting on Use of High-Risk AI

[The National Artificial Intelligence Advisory Committee (NAIAC)]
Law Enforcement Subcommittee (NAIAC-LE Subcommittee)

May 2024

NAIAC MEMBERS

Miriam Vogel, *Chair*
President and CEO of EqualAI

James Manyika, *Vice Chair*
Senior Vice President, Google, President for Research, Technology & Society

Amanda Ballantyne
Director of the AFL-CIO Technology Institute

Jack Clark
Co-founder of Anthropic

David Danks
Professor of Data Science and Philosophy at the University of California, San Diego

Victoria A. Espinel
President and CEO of BSA | The Software Alliance

Paula Goldman
Chief Ethical and Humane Use Officer at Salesforce

Susan Gonzales
Founder and CEO of AIandYou

Janet Haven
Executive Director of Data & Society

Daniel E. Ho
William Benjamin Scott and Luna M. Scott Professor of Law, Professor of Political Science, and Professor of Computer Science (by courtesy), Senior Fellow, Stanford Institute for Human-Centered AI, Stanford University

Ayanna Howard
Dean of Engineering at The Ohio State University

Jon Kleinberg
Professor in the Departments of Computer Science and Information Science at Cornell University

Ramayya Krishnan
W. W. Cooper and Ruth F. Cooper Professor of Management Science and Information Systems, Carnegie Mellon University

Ashley Llorens
Vice President, Distinguished Scientist, and Managing Director at Microsoft Research

Haniyeh Mahmoudian
Global AI Ethicist at DataRobot, Inc.

Christina Montgomery
Chief Privacy & Trust Officer and Vice President at IBM

Liz O'Sullivan
CEO of Vera

Fred Oswald
Professor and Herbert S. Autrey Chair in Social Sciences, Rice University

Trooper Sanders
CEO of Benefits Data Trust

Navrina Singh
Founder and CEO of Credo AI

Swami Sivasubramanian
Vice President for Data and Machine Learning Services at Amazon Web Services

Keith Strier
Vice President for Worldwide AI Initiatives at NVIDIA

Reggie Townsend
Vice President of Data Ethics at SAS Institute

RECOMMENDATION

Office of Management and Budget (OMB) — or another appropriate arm of the Executive branch — should require that law enforcement agencies create and publish annual summary usage reports for safety- or rights-impacting AI to be included in the AI Use Case Inventory.

These reports should include sufficient information for a reader to meaningfully evaluate the extent and nature of the agency's use of the AI tool. Usage reports should include, at a minimum:

- A description of the technology and summary statistics that include the number of times the tool is used, the context and purpose of its use, and counts of the user roles that used the tool. The exact nature of those summary statistics will vary from tool to tool and some examples are included below to help guide the appropriate body in establishing standards
- Total annual costs for the technology, including contributions from non-budgetary sources (e.g., grants, private donations)
- Reporting when and how the tool was used on behalf of other agencies that includes all of the summary information from the previous bullets

Since the form of the summary statistics will depend on how the AI tool is used, the Department of Justice (DOJ) should establish and periodically review the reporting requirements to ensure the statistics reported meet their intended purpose, especially as new tools and uses are reported in the use case inventory. Some examples of summary statistics by use case include:

- For tools such as facial recognition that help identify a person related to an ongoing investigation, summary statistics should include counts by type of case or investigation according to the Uniform Crime Reporting Program's National Incident-Based Reporting System (NIBRS) offense definitions,[1] as well as by source of the image (e.g., cell phone, private surveillance camera, public camera) and the user roll making the search (e.g., police detective, crime lab technician)
- For event detection methods such as gunshot detection, that alert when the system detects a suspicious pattern, summary statistics should include the geographic area where the sensors are located (or

[1] "NIBRS Offense Definitions," Uniform Crime Reporting Program, National Incident-Based Reporting System, 2018, https://ucr.fbi.gov/nibrs/2018/resource-pages/nibrs_offense_definitions-2018.pdf.

other relevant breakdown of sensor placement for things such as cyber crimes or fraud detection) and a breakdown of follow on cases or investigations that were sourced from these methods where relevant, and the number of total alerts made by the system
- For AI-based resource allocation decisions that help agencies spend their time and resources more efficiently by ordering or prioritizing tasks, the relevant geography where the tool was used (such as specific precincts) and the frequency of tool use and nature of allocation decisions made

CONTEXT

In addition to a variety of pre-deployment requirements, OMB's guidance on AI also requires that agencies engage in a number of practices *while using* safety- or rights-impacting AI. Among these requirements, agencies are required to develop ongoing procedures to monitor degradation of the AI's functionality and detect impacts on rights or safety,[2] to mitigate emerging risks to rights and safety,[3] to provide assessment and oversight of AI operators,[4] and more. But these requirements do not mandate that agencies collect or publish basic summary statistics, as in records of how a technology has been used by the agency.

Such summaries of agency use of safety- or rights-impacting AI tools are critical for a variety of internal and external purposes. Internally, agencies can utilize a high-level overview of the purpose for which the tools are used to ensure that the tools are being effectively used against the problem sets for which they were procured or developed. Externally, publishing information about the use of safety- or rights-impacting AI systems can build critical-needed transparency with the public, and help the public validate that systems are being used for the purposes defined in the agency's policy.[5] In most cases, as part of their tool's basic operations, vendors will have the capability of seamlessly producing summary statistics based on the cases

[2] Shalanda Young, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Section 5.iv.D, Office of Management and Budget, March 2024, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[3] "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Section 5.iv.E.
[4] "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence," Section 5.iv.F.
[5] See, for example, the Transparency Portal provided by Flock Safety: https://transparency.flocksafety.com/morgan-hill-ca-pd, https://transparency.flocksafety.com/arlington-pd-wa, https://transparency.flocksafety.com/woodstock-ga-pd, https://transparency.flocksafety.com/alameda-ca-pd.

for which the tools were used and the administrative record keeping necessary for other purposes.

Providing a breakdown of use of safety- or rights- impacting AI tools based on case type or other relevant category balances the need for operational security and confidentiality with a level of granularity that allows the public to assess the impact of these systems and agency adherence to their policies. Building off of an existing framework, such as NIBRS, can help streamline the administrative burden of additional reporting and encourage consistency across agency reports.[6]

[6] "NIBRS Offense Definitions."

ACKNOWLEDGEMENTS

The NAIAC-LE Subcommittee participated in the preparation of this document.

Armando Aguilar
Assistant Chief of Police, Miami Police Department

Anthony Bak
Head of AI, Palantir

Amanda Ballantyne
Director of the AFL-CIO Technology Institute

Jane Bambauer
Director - Marion B. Brechner First Amendment Project, Brechner Eminent Scholar at the College of Journalism and Communications and at Levin College of Law, University of Florida

Esha Bhandari
Deputy Director of the American Civil Liberties Union's Speech, Privacy, and Technology Project

Jennifer Eberhardt
Professor of Organizational Behavior and Psychology, Stanford University

Farhang Heydari
Assistant Professor of Law, Vanderbilt Law School

Benji Hutchinson
Chief Revenue Officer of Rank One Computing

Rashawn Ray
Vice-President and Executive Director of the AIR Equity Initiative

Cynthia Rudin
Professor of Computer Science, Electrical and Computer Engineering, Statistical Science, Mathematics, Biostatistics & Bioinformatics at Duke University

A quorum of the membership of NAIAC reviewed and approved this document.

ABOUT NAIAC

The National Artificial Intelligence Advisory Committee (NAIAC) advises the President and the White House National AI Initiative Office (NAIIO) on the intersection of AI and innovation, competition, societal issues, the economy, law, international relations, and other areas that can and will be impacted by AI in the near and long term. Their work guides the U.S. government in leveraging AI in a uniquely American way — one that prioritizes democratic values and civil liberties, while also increasing opportunity.

NAIAC was established in April 2022 by the William M. (Mac) Thornberry National Defense Authorization Act. It first convened in May 2022. It consists of leading experts in AI across a wide range of domains, from industry to academia to civil society. https://www.ai.gov/naiac/

###