The Future of AI Testing: Insights from the White House Executive Order on AI

November 30, 2023

DLA PIPER

Today’s Speakers

Bennett Borden, JD-MSc

Partner, Chief Data Scientist

DLA Piper

Dr. Sam Tyner-Monroe

Managing Director Accountable AI

DLA Piper

Keith E. Sonderling

Commissioner

Equal Employment Opportunity Commission

Aaron Rieke

Chief of Staff and Attorney Advisor

to Commissioner Bedoya

Federal Trade Commission

White House Executive Order on Safe, Secure, and Trustworthy AI

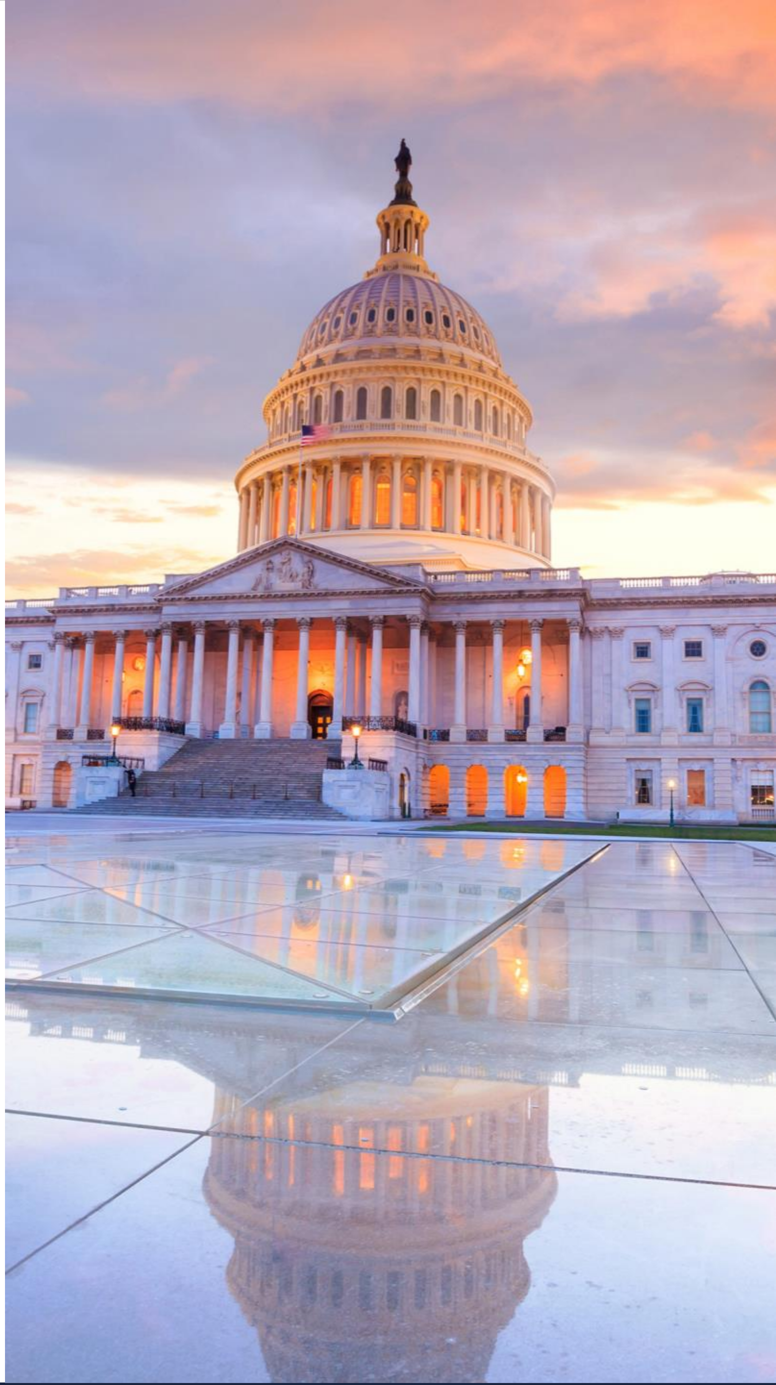
- On October 30, 2023, the White House signed into effect an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.
- The Executive Order makes sweeping mandates to the primary executive departments covering all aspects of the AI lifecycle and impacting most aspects of the economy.
- The Order requires the development of standards, practices, and new regulation for the development and use of AI.

Executive Order AI Principles

- The Order advances eight principles which govern the Federal Government's development and use of AI.
- The eight principles are also meant to guide the oversight of entities operating in the private sector.
- The Order mandates that executive departments and agencies also adhere to the principles when undertaking the actions specified in the Order.

Eight Overarching Principles

- The eight principles are:
  - Ensuring the safety and security of AI technology
  - Promoting innovation and competition
  - Supporting workers
  - Advancing equity and civil rights
  - Protecting consumers, patients, passengers, and students
  - Protecting privacy
  - Advancing Federal Government use of AI
  - Strengthening American leadership abroad



What Agencies Are Implicated by the Order’s Testing Guidance?

The Order requires several entities to create guidance and implement the testing of AI systems, including:

- Department of Health and Human Services
- Consumer Financial Protection Bureau
- Department of Commerce
- Department of Labor
- Department of Energy

What is AI Testing?

- Artificial intelligence testing involves the development of evaluative analytical frameworks and metrics aimed at detecting unwanted behaviors in an AI system.
- Some unwanted behaviors include, but are not limited to, biased outputs, model drift, inaccuracy, unreliability, and security vulnerabilities.

The History of AI Testing

- Testing algorithms for performance has been a part of the development life cycle for as long as algorithmic decision systems have been around.
- Concerns about algorithmic bias can be traced back to at least the 1970s when Joseph Weizenbaum noted that bias could arise from the way programs were coded.
- An early example of algorithmic system testing is the examination of the admissions algorithm employed by St. George’s Hospital Medical School in the 1980s.

What Does the Executive Order Say About AI Testing?

- The Order calls for several agencies to play a role in developing guidance for the testing of AI systems.

- The Order states: *“Testing and evaluations will help ensure that AI systems function as intended, are resilient against misuse or dangerous modifications, are ethically developed and operated in a secure manner, and are compliant with applicable Federal laws and policies.”*

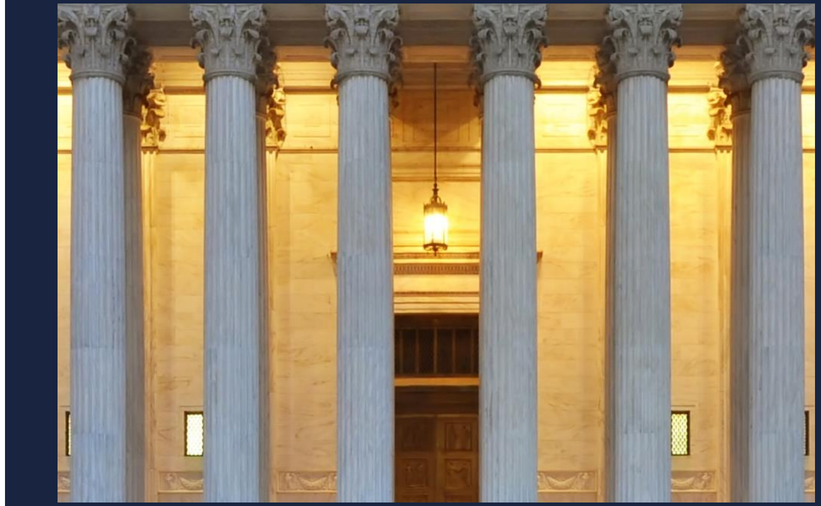
- The Order’s mandates are generally directed at the heads of primary executive agencies.

*“**Independent regulatory agencies** are encouraged … to consider using their **full range of authorities** to protect American consumers from fraud, discrimination, and threats to privacy and to address other risks that may arise from the use of AI, … and to consider **rulemaking**, as well as emphasizing …where **existing regulations** … **apply to AI**, including clarifying the **responsibility of regulated entities** to conduct due diligence on and monitor any third-party AI services, … and … clarifying requirements and expectations related to the **transparency of AI models** and regulated entities’ ability to **explain their use of AI models**.”*

- White House Executive Order on AI, Section 8(a)

Regulatory Perspectives

- How does the Order align with current AI policies?
- What are your primary concerns regarding AI?
- What role will you and your agency play in inter-agency efforts to regulate AI?
- What challenges do you anticipate in regulating emerging AI?
- How might you address the potential for AI to exacerbate existing consumer inequalities?



Who Should Care About AI Testing

- No algorithm or AI system is ever 100% correct, secure, and free of bias.

- All entities developing or deploying AI systems or algorithms should understand that testing is part of the AI life cycle.

- This means that both governmental agencies as well as private entities will need to deploy testing procedures to better eliminate bias and ensure the safety and reliability of their models.

Timelines for Testing

- The Order requires agencies to develop frameworks and testing requirements with differing timeframes for implementation.
- The timeframes for the Order’s mandates range from 90 – 365 days.

* Note
* runs bef
* as indicating
*/
function incode_starter_se
/* Make theme available for trans
* Translations can be filed in the
* If you're building a theme based on
* to change 'incode_starter' to the
et.xml

Selected Timelines

- **Within 90 days**:
  - The Secretary of Commerce to require developers of foundation models to report to the Federal Government on the model's performance in relevant AI red-team testing;
  - The Assistant Attorney General in charge of the Civil Rights Division to convene a meeting of the heads of Federal civil rights offices to discuss prevention of discrimination in the use of automated systems, including algorithmic discrimination.
- **Within 180 days**:
  - The Secretary of Agriculture to issue guidance on use of AI in benefits programs, including analysis of whether algorithmic systems in use by benefit programs achieve equitable outcomes;
  - The Secretary of Transportation to direct Federal Advisory Committees to provide advice on the safe and responsible use of AI in transportation.
- **Within 365 days**:
  - The Secretary of Education to develop resources with relevant stakeholders which address safe, responsible, and nondiscriminatory uses of AI in education, including the impact AI systems have on vulnerable and underserved communities;
  - The Secretary of Labor to publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems;

Healthcare Testing

- The Order instructs Health and Human Services to foster the **responsible use of AI in healthcare and benefits administration**.

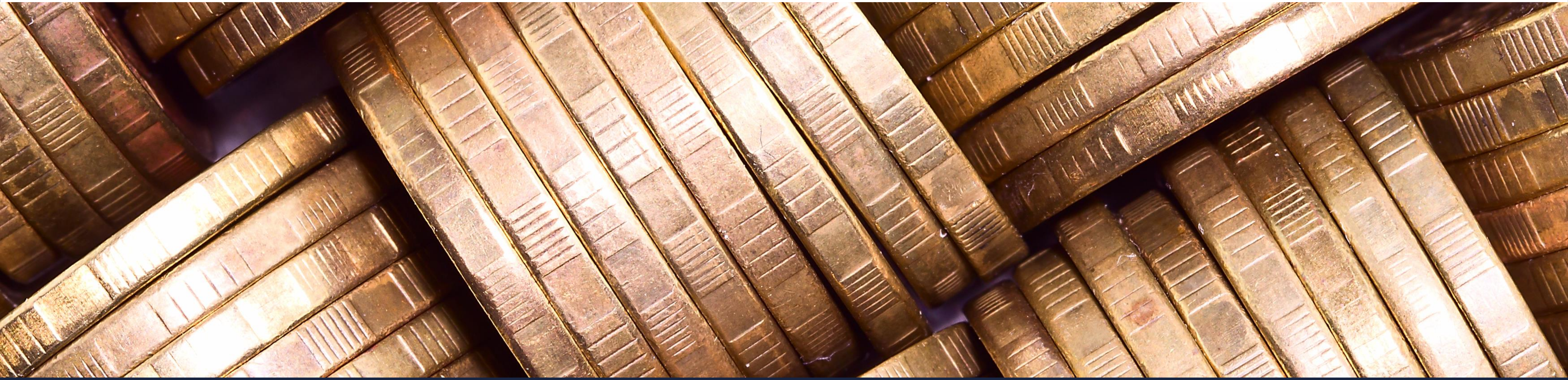
- This includes the establishment of an HHS AI Task Force to, *"develop a strategic plan that includes policies and frameworks […] on* ***responsible deployment and use of AI and AI-enabled technologies in the health and human services sector*** *[including] long-term safety and real-world performance monitoring of AI-enabled technologies."*

- The Order mandates HHS to create an AI safety program to establish *"a common framework for approaches to identifying and capturing* ***clinical errors resulting from AI deployed in healthcare*** *settings as well as specification for a central tracking repository for associated* ***incidents that cause harm, including through bias or discrimination, to patients, caregivers, or other parties****."*

Financial Services Testing

- The Federal Housing Finance Agency and the Consumer Financial Protection Bureau are *"encouraged to require their respective regulated entities […] to use the appropriate methodologies including AI tools to ensure compliance with federal law."*

- This **includes testing and evaluating underwriting models for bias or disparities** that affect protected groups and automating collateral-valuation and appraisal processing in ways that minimize bias.



Employment Testing

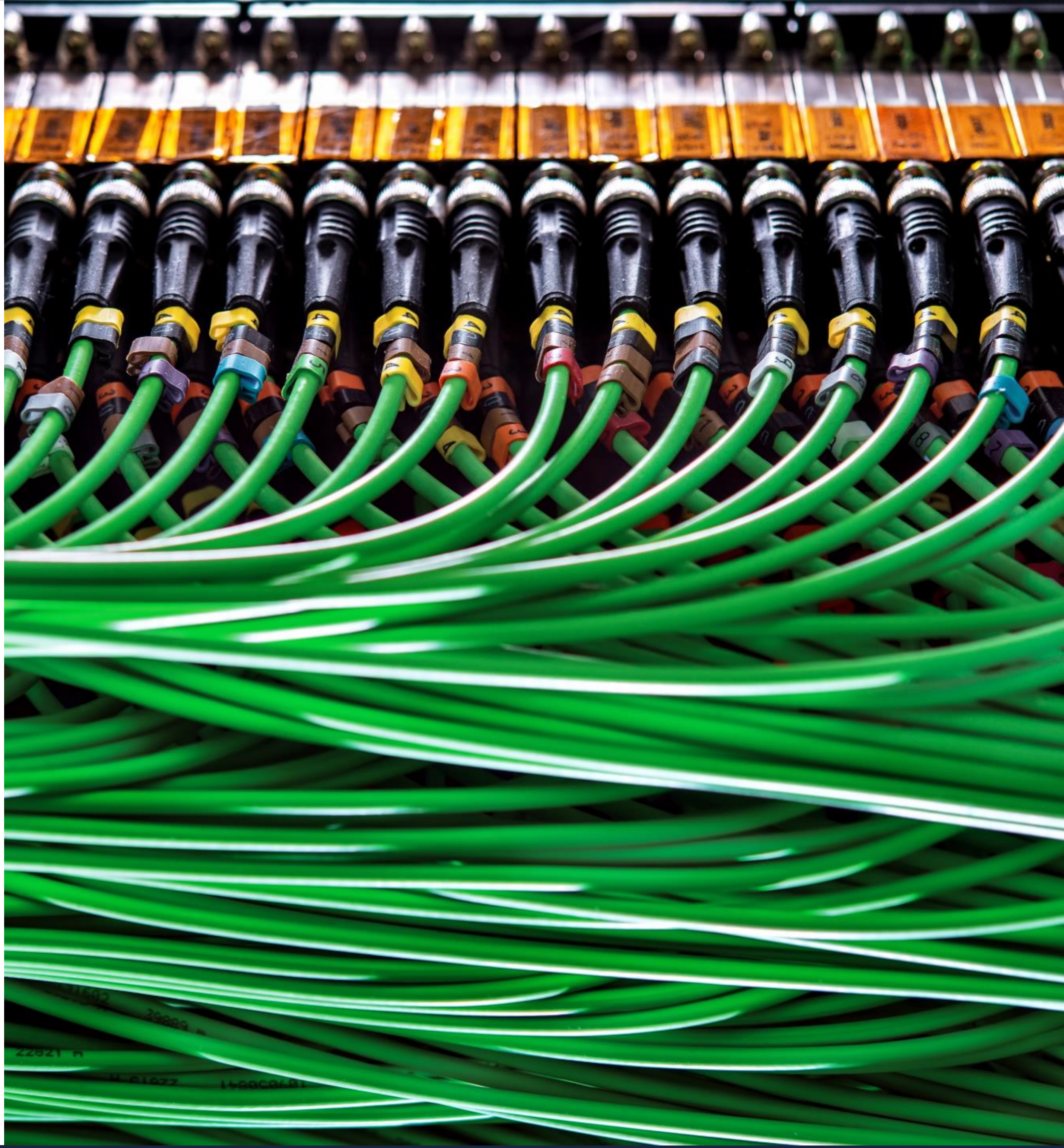
- The Order states the Department of Labor has a responsibility to *“prevent unlawful discrimination from AI used for hiring”* and *“publish guidance for Federal contractors regarding nondiscrimination in hiring involving AI and other technology-based hiring systems.”*

- It is expected that testing AI systems for unintended bias will be an integral part of the Department of Labor’s guidance on nondiscriminatory hiring involving AI.

Generative AI Testing

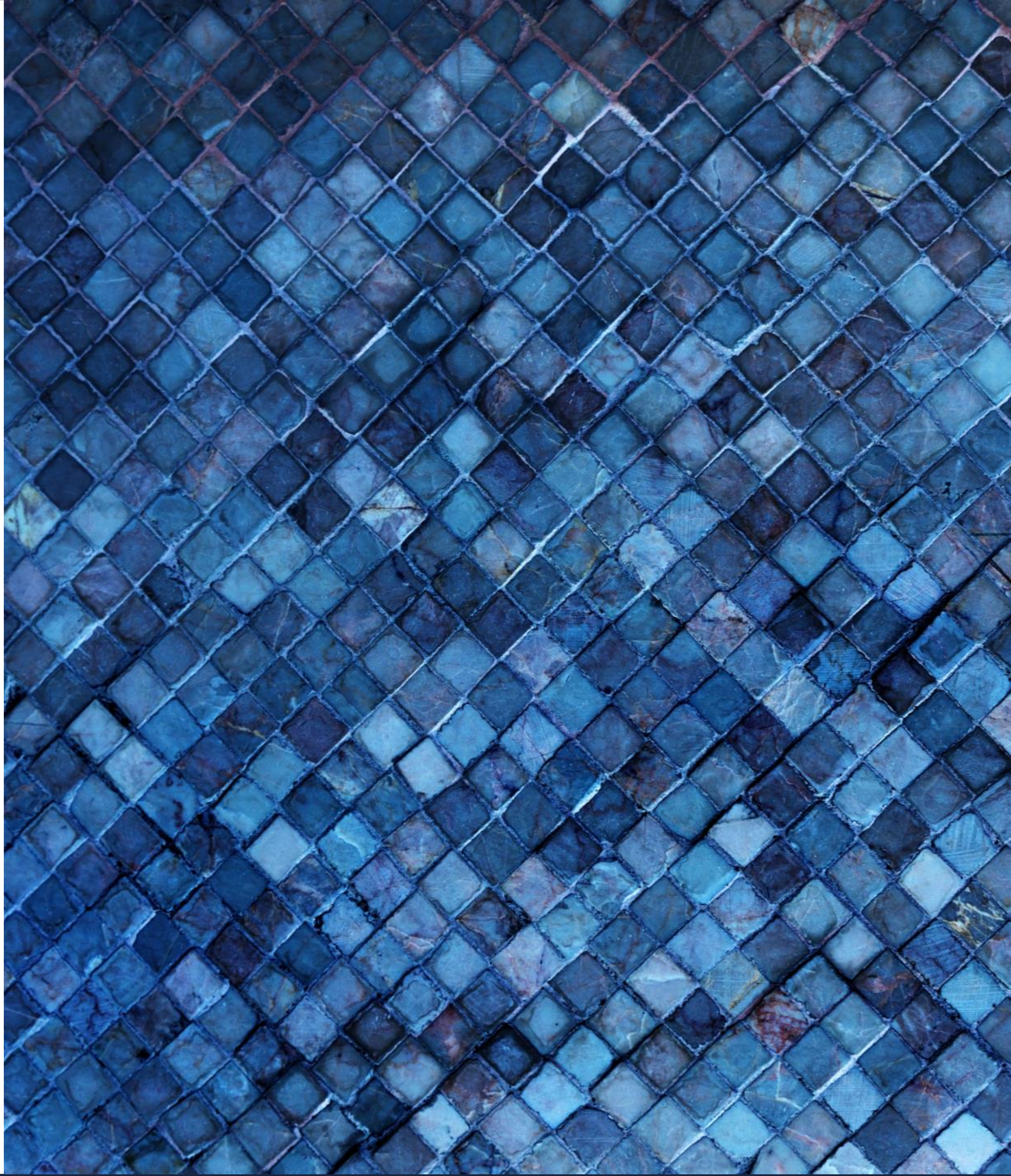
- The Department of Energy is required to create AI testbeds for foundation models, which are, *"facilit[ies] or mechanism[s] equipped for conducting…testing of tools and technologies, including AI and privacy-enhancing technologies, to help evaluate the functionality, usability, and performance of those tools or technologies."*

- The Department of Commerce is required to collect reports from companies developing foundation models on red-team testing results and other security testing measures.

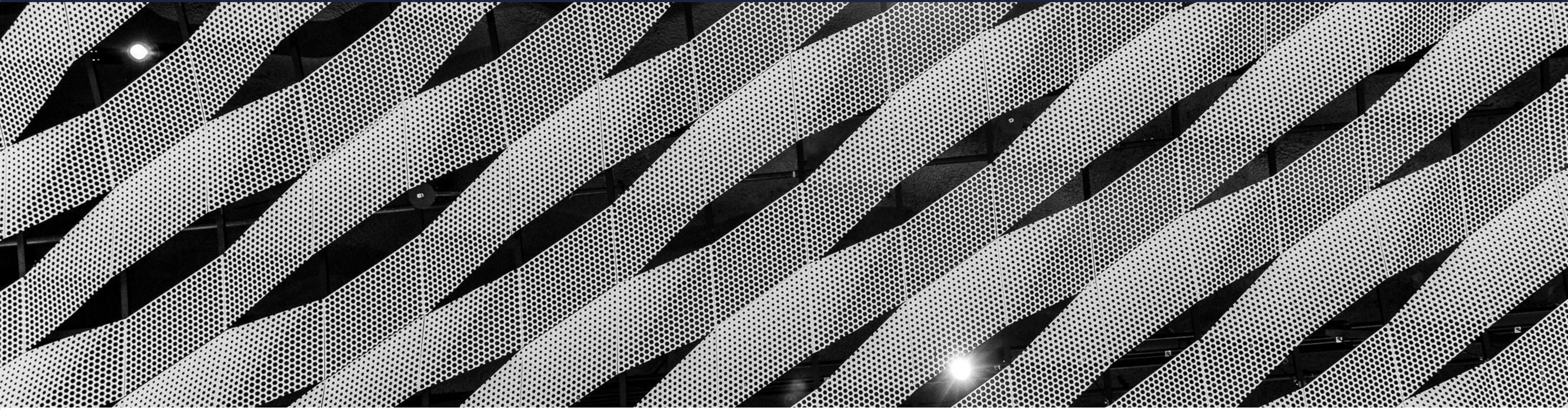


Methodology

- Identify higher risk AI systems for testing (consumer-facing, automated decisions, etc.)
  - What is the business purpose?
  - What is the technical execution?
- How does the system distinguish between people? How does that affect their output from the system?
- Can we identify a statistically significant difference between outputs across members of protected classes?
- If so, can we identify the cause and mitigate it or demonstrate its utility?



Final Thoughts



Next Steps

For more information these topics, please contact the individuals below:

Bennett Borden
Partner, Chief Data Scientist
Bennett.Borden@us.dlapiper.com

Dr. Sam Tyner-Monroe
Managing Director Accountable AI
Sam.Tyner-Monroe@us.dlapiper.com

Thank you.

All information, content, and materials contained in this publication/program are for informational purposes only. This publication/program is intended to be a general overview of the subjects discussed and does not create a lawyer-client relationship. Statements and opinions are those of the individual speakers, authors, and participants and do not necessarily reflect the policies or opinions of DLA Piper LLP (US). The information contained in this publication/program is not, and should not be used as, a substitute for legal advice. No reader should act, or refrain from acting, with respect to any particular legal matter on the basis of this publication/program and should seek legal advice from counsel in the relevant jurisdiction. This publication and the program may qualify as "Lawyer Advertising," requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome. DLA Piper LLP (US)