

Ch_496_sb0818E.pdf

Uploaded by: Katie Fry Hester

Position: FAV

Chapter 496

(Senate Bill 818)

AN ACT concerning

**Information Technology – Artificial Intelligence – Policies and Procedures
(Artificial Intelligence Governance Act of 2024)**

FOR the purpose of requiring each unit of State government to conduct a certain annual data inventory, a certain ~~annual~~ inventory of systems that employ artificial intelligence, and a certain impact assessment on or before a certain date; ~~requiring prohibiting~~ the Department of Information Technology from making certain information publicly available under certain circumstances to conduct ongoing monitoring of certain systems under certain circumstances; requiring the Department of Information Technology, in consultation with the Governor's Artificial Intelligence Subcabinet of the Governor's Executive Council, to adopt policies and procedures concerning the development, procurement, ~~implementation~~ deployment, use, and assessment of systems that employ artificial intelligence by units of State government; prohibiting a unit of State government from ~~implementing~~ deploying or using a system that employs artificial intelligence under certain circumstances beginning on a certain date; requiring a unit of State government to conduct certain regular impact assessments under certain circumstances; exempting the Office of the Attorney General, the Comptroller, the Treasurer, and certain public institutions of higher education from certain provisions; establishing the ~~Governor's Artificial Intelligence Subcabinet of the Governor's Executive Council~~; establishing competitive proof of concept procurement as a formal competitive procurement method for the procurement of certain products and services; ~~exempting certain competitive proof of concept procurements from oversight by the Board of Public Works~~; requiring the Department of General Services, in consultation with the Department of Information Technology, to develop certain policies and procedures for the development and implementation of competitive proof of concept procurements; requiring the Subcabinet to develop a certain roadmap; and generally relating to the use of artificial intelligence by units of State government.

BY repealing and reenacting, without amendments,

Article – State Finance and Procurement

Section 3.5–101(a), (c), (d), and (f)

Annotated Code of Maryland

(2021 Replacement Volume and 2023 Supplement)

BY repealing and reenacting, with amendments,

Article – State Finance and Procurement

~~Section 3.5–301, 3.5–303(a), and 12–101~~ Section 3.5–301 and 3.5–303(a)

Annotated Code of Maryland

(2021 Replacement Volume and 2023 Supplement)

BY adding to

Article – State Finance and Procurement

Section 3.5–318; 3.5–801 through ~~3.5–805~~ 3.5–806 to be under the new subtitle “Subtitle 8. Artificial Intelligence”; and 13–116

Annotated Code of Maryland

(2021 Replacement Volume and 2023 Supplement)

Preamble

WHEREAS, Artificial intelligence is transforming society and work, and the pace of that change will present new opportunities and risks for the State’s residents, workers, and economy; and

WHEREAS, The State must ensure the responsible, ethical, beneficial, and trustworthy use of artificial intelligence in State government; and

WHEREAS, The State is home to a rich and growing artificial intelligence ecosystem of academic, industry, government, and civil society experts, researchers, builders, organizers, and stakeholders; and

WHEREAS, To foster an environment for innovation while respecting individuals, employees, and civil rights, as artificial intelligence technologies are developed and evolve, the technologies should be analyzed and monitored by government officials, industry experts, consumer protection advocates, and other stakeholders; and

WHEREAS, Given the rapid rate of change in artificial intelligence technologies and industry, the State must chart a principled yet adaptable, pragmatic path forward, so that the technologies’ benefits can be confidently harnessed on behalf of Marylanders and in service of the Governor’s mission to Leave No One Behind; and

WHEREAS, Leaders across State government share a common interest in establishing effective artificial intelligence governance and are committed to working together to develop the legal and policy framework for its responsible use in the State; and

WHEREAS, Automated systems should be safe and effective, developed with consultation from diverse communities, stakeholders, and domain experts to identify concerns, risks, and potential impacts of the systems; and

WHEREAS, Designers, developers, and deployers of automated systems should take proactive and continuous measures to protect individuals and communities from algorithmic discrimination and to use and design systems in an equitable way; and

WHEREAS, Designers, developers, and deployers of automated systems should seek permission and respect decisions regarding collection, use, access, transfer, and deletion of data in appropriate ways and to the greatest extent possible; where not possible, alternative privacy by design safeguards should be used; and

WHEREAS, Designers, developers, and deployers of automated systems should provide generally accessible plain language documentation including clear descriptions of the overall system functioning and the role automation plays, notice that such systems are in use, the individual or organization responsible for the system, and explanations of outcomes that are clear, timely, and accessible; and

WHEREAS, Designers, developers, and deployers of automated systems should consider the specific types of actions for which a human alternative is appropriate, commensurate with the magnitude of the action and risk of harm, along with the extent to which a human alternative would be beneficial to individuals and the public interest; now, therefore,

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND,
That the Laws of Maryland read as follows:

Article – State Finance and Procurement

3.5–101.

(a) In this title the following words have the meanings indicated.

(c) “Department” means the Department of Information Technology.

(d) “Secretary” means the Secretary of Information Technology.

(f) “Unit of State government” means an agency or unit of the Executive Branch of State government.

3.5–301.

(a) In this subtitle the following words have the meanings indicated.

(B) “ARTIFICIAL INTELLIGENCE” HAS THE MEANING STATED IN § 3.5–801 OF THIS TITLE.

[(b)] (C) “Cybersecurity” means processes or capabilities wherein systems, communications, and information are protected and defended against damage, unauthorized use or modification, and exploitation.

[(c)] (D) “Cybersecurity strategy” means a vision, a plan of action, or guiding principles.

[(d)] (E) (1) “Development” means all expenditures for a new information technology system or an enhancement to an existing system including system:

- (i) planning;
- (ii) creation;
- (iii) installation;
- (iv) testing; and
- (v) initial training.

(2) “Development” does not include:

(i) ongoing operating costs, software or hardware maintenance, routine upgrades, or modifications that merely allow for a continuation of the existing level of functionality; or

(ii) expenditures made after a new or enhanced system has been legally accepted by the user and is being used for the business process for which it was intended.

[(e)] (F) “Fund” means the Major Information Technology Development Project Fund.

[(f)] (G) “Information technology” means all electronic information processing, including:

- (1) maintenance;
- (2) telecommunications;
- (3) hardware;
- (4) software; and
- (5) associated services.

[(g)] (H) “Information technology services” means information provided by electronic means by or on behalf of a unit of State government.

[(h)] (I) “Major information technology development project” means any information technology development project that meets one or more of the following criteria:

- (1) the estimated total cost of development equals or exceeds \$1,000,000;

(2) the project is undertaken to support a critical business function associated with the public health, education, safety, or financial well-being of the citizens of Maryland; or

(3) the Secretary determines that the project requires the special attention and consideration given to a major information technology development project due to:

- (i) the significance of the project's potential benefits or risks;
- (ii) the impact of the project on the public or local governments;
- (iii) the public visibility of the project; or
- (iv) other reasons as determined by the Secretary.

[(i)] (J) "Master plan" means the statewide information technology master plan and statewide cybersecurity strategy.

[(j)] (K) "Nonvisual access" means the ability, through keyboard control, synthesized speech, Braille, or other methods not requiring sight to receive, use, and manipulate information and operate controls necessary to access information technology in accordance with standards adopted under § 3.5–303(b) of this subtitle.

[(k)] (L) "Resource sharing" means the utilization of a State resource by private industry in exchange for the provision to the State of a communication service or other consideration.

[(l)] (M) "Systems development life cycle plan" means a plan that defines all actions, functions, or activities to be performed by a unit of State government in the definition, planning, acquisition, development, testing, implementation, operation, enhancement, and modification of information technology systems.

3.5–303.

(a) The Secretary is responsible for carrying out the following duties:

(1) developing, maintaining, revising, and enforcing information technology policies, procedures, and standards;

(2) providing technical assistance, advice, and recommendations to the Governor and any unit of State government concerning information technology matters;

(3) reviewing the annual project plan for each unit of State government to make information and services available to the public over the Internet;

(4) developing and maintaining a statewide information technology master plan that will:

(i) centralize the management and direction of information technology policy within the Executive Branch of State government under the control of the Department;

(ii) include all aspects of State information technology including telecommunications, security, data processing, and information management;

(iii) consider interstate transfers as a result of federal legislation and regulation;

(iv) ensure that the State information technology plan and related policies and standards are consistent with State goals, objectives, and resources, and represent a long-range vision for using information technology to improve the overall effectiveness of State government;

(v) include standards to assure nonvisual access to the information and services made available to the public over the Internet; and

(vi) allows a State agency to maintain the agency's own information technology unit that provides for information technology services to support the mission of the agency;

(5) developing and maintaining a statewide cybersecurity strategy that will:

(i) centralize the management and direction of cybersecurity strategy within the Executive Branch of State government under the control of the Department; and

(ii) serve as the basis for budget allocations for cybersecurity preparedness for the Executive Branch of State government;

(6) adopting by regulation and enforcing nonvisual access standards to be used in the procurement of information technology services by or on behalf of units of State government in accordance with subsection (c) of this section;

(7) in consultation with the Maryland Cybersecurity Coordinating Council, advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions under the control of the governing boards of the public institutions of higher education;

(8) advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy;

(9) in consultation with the Maryland Cybersecurity Coordinating Council, developing guidance on consistent cybersecurity strategies for counties, municipal corporations, school systems, and all other political subdivisions of the State;

(10) upgrading information technology and cybersecurity-related State government infrastructure; [and]

(11) annually evaluating:

(i) the feasibility of units of State government providing public services using artificial intelligence, machine learning, commercial cloud computer services, device-as-a-service procurement models, and other emerging technologies; and

(ii) the development of data analytics capabilities to enable data-driven policymaking by units of State government; AND

(12) CONDUCTING INVENTORIES ~~AND ONGOING ASSESSMENTS~~ OF SYSTEMS THAT EMPLOY ARTIFICIAL INTELLIGENCE THAT ARE USED BY A UNIT OF STATE GOVERNMENT AS REQUIRED UNDER ~~§ 3.5-318 OF THIS SUBTITLE~~ § 3.5-803 OF THIS TITLE.

3.5-318.

(A) ON OR BEFORE DECEMBER 1, 2024, AND ANNUALLY THEREAFTER, EACH UNIT OF STATE GOVERNMENT SHALL CONDUCT A DATA INVENTORY THAT IDENTIFIES DATA THAT MEETS THE CRITERIA ESTABLISHED BY THE CHIEF DATA OFFICER AND THAT IS:

(1) (I) NECESSARY FOR THE OPERATION OF THE UNIT; OR

(II) OTHERWISE REQUIRED TO BE COLLECTED:

1. AS A CONDITION TO RECEIVE FEDERAL FUNDS; OR

2. BY FEDERAL OR STATE LAW; AND

(2) IN A FORM PRESCRIBED BY THE CHIEF DATA OFFICER, INCLUDING WHEN THE DATA IS USED IN ARTIFICIAL INTELLIGENCE.

(B) THE DEPARTMENT SHALL DEVELOP AND PUBLISH GUIDANCE ON THE POLICIES AND PROCEDURES FOR THE INVENTORY.

SUBTITLE 8. ARTIFICIAL INTELLIGENCE.

3.5–801.

(A) IN THIS SUBTITLE THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED.

(B) (1) “ALGORITHMIC DECISION SYSTEM” MEANS A COMPUTATIONAL PROCESS THAT FACILITATES DECISION MAKING.

(2) “ALGORITHMIC DECISION SYSTEM” INCLUDES DECISIONS DERIVED FROM MACHINES, STATISTICS, FACIAL RECOGNITION, AND DECISIONS ON PAPER.

(C) “ARTIFICIAL INTELLIGENCE” MEANS A MACHINE–BASED SYSTEM THAT:

(1) CAN, FOR A GIVEN SET OF HUMAN–DEFINED OBJECTIVES, MAKE PREDICTIONS, RECOMMENDATIONS, OR DECISIONS INFLUENCING REAL OR VIRTUAL ENVIRONMENTS;

(2) USES MACHINE AND HUMAN–BASED INPUTS TO PERCEIVE REAL AND VIRTUAL ENVIRONMENTS AND ABSTRACTS THOSE PERCEPTIONS INTO MODELS THROUGH ANALYSIS IN AN AUTOMATED MANNER; AND

(3) USES MODEL INFERENCE TO FORMULATE OPTIONS FOR INFORMATION OR ACTION.

~~(D) “HIGH RISK” MEANS AN ACT THAT IS LIKELY TO:~~

~~(1) RESULT IN ANY UNLAWFUL DISCRIMINATION;~~

~~(2) HAVE AN UNLAWFUL DISPARATE IMPACT ON ANY INDIVIDUAL OR GROUP OF INDIVIDUALS ON THE BASIS OF ANY ACTUAL OR PERCEIVED CHARACTERISTIC; OR~~

~~(3) HAVE A NEGATIVE IMPACT ON THE HEALTH, SAFETY, OR WELL BEING OF AN INDIVIDUAL.~~

~~(E) (D) “IMPACT ASSESSMENT” MEANS A DOCUMENTED RISK BASED EVALUATION OF A SYSTEM THAT EMPLOYS RIGHTS IMPACTING OR SAFETY IMPACTING ARTIFICIAL INTELLIGENCE.~~

(D) (1) “HIGH-RISK ARTIFICIAL INTELLIGENCE” MEANS ARTIFICIAL INTELLIGENCE THAT IS A RISK TO INDIVIDUALS OR COMMUNITIES, AS DEFINED

UNDER REGULATIONS ADOPTED BY THE DEPARTMENT IN CONSULTATION WITH THE GOVERNOR'S ARTIFICIAL INTELLIGENCE SUBCABINET.

(2) "HIGH-RISK ARTIFICIAL INTELLIGENCE" INCLUDES RIGHTS-IMPACTING ARTIFICIAL INTELLIGENCE AND SAFETY-IMPACTING ARTIFICIAL INTELLIGENCE.

(E) "IMPACT ASSESSMENT" MEANS AN ASSESSMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS MADE UNDER REGULATIONS ADOPTED BY THE DEPARTMENT IN CONSULTATION WITH THE GOVERNOR'S ARTIFICIAL INTELLIGENCE SUBCABINET AND REQUIRED UNDER § 3.5-803 OF THIS SUBTITLE.

~~(E)~~ (F) "PUBLIC SENIOR HIGHER EDUCATION INSTITUTION" MEANS:

(1) THE CONSTITUENT INSTITUTIONS OF THE UNIVERSITY SYSTEM OF MARYLAND AND THE UNIVERSITY OF MARYLAND CENTER FOR ENVIRONMENTAL SCIENCE;

(2) MORGAN STATE UNIVERSITY; OR

(3) ST. MARY'S COLLEGE OF MARYLAND.

~~(F)~~ (G) "RIGHTS-IMPACTING ARTIFICIAL INTELLIGENCE" MEANS ARTIFICIAL INTELLIGENCE WHOSE OUTPUT SERVES AS A BASIS FOR DECISION OR ACTION THAT HAS A LEGAL, MATERIAL, OR SIMILARLY SIGNIFICANT EFFECT ON AN INDIVIDUAL'S OR COMMUNITY'S;

~~(1) CIVIL RIGHTS, CIVIL LIBERTIES, OR PRIVACY, INCLUDING FREEDOM OF SPEECH, VOTING, HUMAN AUTONOMY, AND PROTECTIONS FROM DISCRIMINATION, EXCESSIVE PUNISHMENT, AND UNLAWFUL SURVEILLANCE;~~

~~(2) EQUAL OPPORTUNITIES, INCLUDING EQUITABLE ACCESS TO EDUCATION, HOUSING, CREDIT, EMPLOYMENT, AND OTHER SITUATIONS WHERE CIVIL RIGHTS AND EQUAL OPPORTUNITY PROTECTIONS APPLY; OR~~

~~(3) ACCESS TO CRITICAL RESOURCES OR SERVICES, INCLUDING HEALTH CARE, FINANCIAL SERVICES, SOCIAL SERVICES, TRANSPORTATION, NONDECEPTIVE INFORMATION ABOUT GOODS AND SERVICES, AND GOVERNMENT BENEFITS OR PRIVILEGES. IS SIGNIFICANTLY LIKELY TO AFFECT CIVIL RIGHTS, CIVIL LIBERTIES, EQUAL OPPORTUNITIES, ACCESS TO CRITICAL RESOURCES, OR PRIVACY.~~

~~(G)~~ (H) "SAFETY-IMPACTING ARTIFICIAL INTELLIGENCE" MEANS ARTIFICIAL INTELLIGENCE THAT HAS THE POTENTIAL TO MEANINGFULLY

~~SIGNIFICANTLY IMPACT THE SAFETY OF INDIVIDUALS AND COMMUNITIES REGARDING:~~

~~(1) HUMAN LIFE OR WELL-BEING, INCLUDING LOSS OF LIFE, SERIOUS INJURY, BODILY HARM, BIOLOGICAL OR CHEMICAL WEAPONS, OCCUPATIONAL HAZARDS, HARASSMENT OR ABUSE, OR MENTAL HEALTH;~~

~~(2) THE CLIMATE OR THE ENVIRONMENT, INCLUDING IRREVERSIBLE OR SIGNIFICANT ENVIRONMENTAL DAMAGE;~~

~~(3) CRITICAL INFRASTRUCTURE, INCLUDING THE INFRASTRUCTURE FOR VOTING AND PROTECTING THE INTEGRITY OF ELECTIONS; OR~~

~~(4) STRATEGIC ASSETS OR RESOURCES, INCLUDING INTELLECTUAL PROPERTY, OF HUMAN LIFE, WELL-BEING, OR CRITICAL INFRASTRUCTURE.~~

3.5-802.

~~(A) THIS SUBTITLE APPLIES TO EACH PUBLIC SENIOR HIGHER EDUCATION INSTITUTION AND BALTIMORE CITY COMMUNITY COLLEGE IN A PARTNERSHIP FOR THE DEVELOPMENT, PROCUREMENT, DEPLOYMENT, OR USE OF ARTIFICIAL INTELLIGENCE WITH A UNIT OF STATE GOVERNMENT.~~

~~(B) EXCEPT AS PROVIDED IN § 3.5-804(D) OF THIS SUBTITLE, THIS SUBTITLE DOES NOT APPLY TO ARTIFICIAL INTELLIGENCE DEPLOYED BY PUBLIC SENIOR HIGHER EDUCATION INSTITUTIONS OR BALTIMORE CITY COMMUNITY COLLEGE USED SOLELY FOR A RESEARCH OR ACADEMIC PURPOSE, INCLUDING IN A PARTNERSHIP FOR THE DEVELOPMENT, PROCUREMENT, DEPLOYMENT, OR USE OF ARTIFICIAL INTELLIGENCE WITH A UNIT OF STATE GOVERNMENT.~~

~~(C) A PUBLIC SENIOR HIGHER EDUCATION INSTITUTION OR BALTIMORE CITY COMMUNITY COLLEGE SHALL ESTABLISH POLICIES AND PROCEDURES THAT ARE FUNCTIONALLY COMPATIBLE WITH THE POLICIES AND PROCEDURES ADOPTED UNDER § 3.5-804(A) OF THIS SUBTITLE FOR ARTIFICIAL INTELLIGENCE DEPLOYED FOR AN OPERATIONS-RELATED PURPOSE.~~

~~(A) (1) EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, THIS SUBTITLE DOES NOT APPLY TO:~~

~~(I) THE OFFICE OF THE ATTORNEY GENERAL;~~

~~(II) THE COMPTROLLER; OR~~

(III) THE STATE TREASURER.

(2) ON OR BEFORE JUNE 1, 2025, EACH ENTITY LISTED UNDER PARAGRAPH (1) OF THIS SUBSECTION SHALL ESTABLISH POLICIES AND PROCEDURES THAT ARE FUNCTIONALLY COMPATIBLE WITH THE POLICIES AND PROCEDURES ADOPTED UNDER § 3.5-804(A) OF THIS SUBTITLE FOR THE DEVELOPMENT, PROCUREMENT, DEPLOYMENT, USE, AND ONGOING ASSESSMENT OF SYSTEMS THAT EMPLOY HIGH-RISK ARTIFICIAL INTELLIGENCE.

(B) (1) EXCEPT AS PROVIDED IN PARAGRAPH (2) OF THIS SUBSECTION, THIS SUBTITLE APPLIES TO EACH PUBLIC SENIOR HIGHER EDUCATION INSTITUTION AND BALTIMORE CITY COMMUNITY COLLEGE.

(2) THIS SUBTITLE DOES NOT APPLY TO ARTIFICIAL INTELLIGENCE DEPLOYED BY A PUBLIC SENIOR HIGHER EDUCATION INSTITUTION OR BALTIMORE CITY COMMUNITY COLLEGE THAT IS USED SOLELY FOR A RESEARCH OR ACADEMIC PURPOSE, INCLUDING IN PARTNERSHIP WITH A UNIT OF STATE GOVERNMENT FOR THE DEVELOPMENT, PROCUREMENT, DEPLOYMENT, OR USE OF ARTIFICIAL INTELLIGENCE.

(3) ON OR BEFORE JUNE 1, 2025, EACH PUBLIC SENIOR HIGHER EDUCATION INSTITUTION AND BALTIMORE CITY COMMUNITY COLLEGE SHALL ESTABLISH POLICIES AND PROCEDURES THAT ARE FUNCTIONALLY COMPATIBLE WITH THE POLICIES AND PROCEDURES ADOPTED UNDER § 3.5-804(A) OF THIS SUBTITLE FOR THE DEVELOPMENT, PROCUREMENT, DEPLOYMENT, USE, AND ONGOING ASSESSMENT OF SYSTEMS THAT EMPLOY HIGH-RISK ARTIFICIAL INTELLIGENCE USED SOLELY FOR A RESEARCH OR ACADEMIC PURPOSE.

(4) ON OR BEFORE SEPTEMBER 1, 2025, AND EACH YEAR THEREAFTER, EACH PUBLIC SENIOR HIGHER EDUCATION INSTITUTION AND BALTIMORE CITY COMMUNITY COLLEGE SHALL SUBMIT TO THE DEPARTMENT A REPORT ON ALL HIGH-RISK ARTIFICIAL INTELLIGENCE PROCURED AND DEPLOYED FOR A RESEARCH OR ACADEMIC PURPOSE.

3.5-803.

(A) ON OR BEFORE DECEMBER 1, ~~2024~~ 2025, AND ~~ANNUALLY~~ REGULARLY THEREAFTER, EACH UNIT OF STATE GOVERNMENT SHALL:

(1) CONDUCT AN INVENTORY OF SYSTEMS THAT EMPLOY ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE; AND

(2) PROVIDE THE INVENTORY TO THE DEPARTMENT IN A FORMAT REQUIRED BY THE DEPARTMENT.

(B) FOR EACH SYSTEM, THE INVENTORY REQUIRED BY THIS SECTION SHALL INCLUDE:

- (1) THE NAME OF THE SYSTEM;**
- (2) THE VENDOR THAT PROVIDED THE SYSTEM, IF APPLICABLE;**
- (3) A DESCRIPTION OF THE CAPABILITIES OF THE SYSTEM;**
- (4) A STATEMENT OF THE PURPOSE AND THE INTENDED USES OF THE SYSTEM;**
- (5) WHETHER THE SYSTEM UNDERWENT AN IMPACT ASSESSMENT PRIOR TO BEING ~~IMPLEMENTED~~ DEPLOYED;**
- (6) WHETHER THE SYSTEM IS USED TO INDEPENDENTLY MAKE A DECISION OR JUDGMENT OR TO INFORM OR SUPPORT A DECISION OR JUDGMENT DETERMINED BY THE DEPARTMENT TO INVOLVE ~~A HIGH-RISK ACTION RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE; AND**
- (7) ~~A DETERMINATION OF THE RISK THAT USE OF A SYSTEM MAY BE HIGH-RISK~~ SUMMARY OF THE RESULTS OF THE MOST RECENT IMPACT ASSESSMENT.**

(C) THE DEPARTMENT SHALL MAKE ~~EACH INVENTORY REQUIRED BY THIS SECTION~~ AN AGGREGATED STATEWIDE INVENTORY PUBLICLY AVAILABLE ON ITS WEBSITE.

(D) (1) THE DEPARTMENT MAY NOT MAKE PUBLICLY AVAILABLE ON THE DEPARTMENT'S WEBSITE INFORMATION FROM THE INVENTORIES REQUIRED BY THIS SECTION THAT RELATE TO THE SAFETY AND SECURITY OF STATE SYSTEMS IF THE PUBLICATION OF THE INFORMATION IS LIKELY TO COMPROMISE THE SECURITY OR INTEGRITY OF THE SYSTEM.

(2) ON REQUEST, THE DEPARTMENT SHALL PROVIDE TO THE GOVERNOR, MEMBERS OF THE GENERAL ASSEMBLY, AND LAW ENFORCEMENT THE INFORMATION DESCRIBED IN PARAGRAPH (1) OF THIS SUBSECTION.

(E) (1) ON OR BEFORE ~~FEBRUARY 1, 2025,~~ DECEMBER 31, 2025 ~~2026~~, EACH UNIT OF STATE GOVERNMENT SHALL CONDUCT AN IMPACT ASSESSMENT OF A

SYSTEM PROCURED ON OR AFTER FEBRUARY 1, ~~2025~~ 2026, THAT INVOLVES A HIGH-RISK ACTION ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE.

(2) ON OR BEFORE ~~FEBRUARY~~ JULY 1, 2027, EACH UNIT OF STATE GOVERNMENT SHALL CONDUCT AN IMPACT ASSESSMENT OF A SYSTEM PROCURED BEFORE FEBRUARY 1, ~~2025~~ 2026, THAT INVOLVES ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE.

~~3.5-803.~~ 3.5-804.

(A) ON OR BEFORE DECEMBER 1, 2024, THE DEPARTMENT, IN CONSULTATION WITH THE GOVERNOR'S ARTIFICIAL INTELLIGENCE SUBCABINET, SHALL ADOPT POLICIES AND PROCEDURES CONCERNING THE DEVELOPMENT, PROCUREMENT, ~~IMPLEMENTATION~~ DEPLOYMENT, USE, AND ONGOING ASSESSMENT OF SYSTEMS THAT EMPLOY ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE BY A UNIT OF STATE GOVERNMENT.

(B) THE POLICIES AND PROCEDURES REQUIRED BY SUBSECTION (A) OF THIS SECTION SHALL:

(1) SUBJECT TO ANY OTHER APPLICABLE LAW, GOVERN THE PROCUREMENT, ~~IMPLEMENTATION~~ DEPLOYMENT, AND ONGOING ASSESSMENT OF SYSTEMS THAT EMPLOY ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE BY A UNIT OF STATE GOVERNMENT;

~~(2) BE SUFFICIENT TO ENSURE THAT THE USE OF ANY SYSTEM THAT EMPLOYS ARTIFICIAL INTELLIGENCE BY ANY UNIT OF STATE GOVERNMENT IS NOT HIGH-RISK;~~

~~(3) REQUIRE EACH UNIT OF STATE GOVERNMENT TO ASSESS THE LIKELY IMPACT OF ANY SYSTEM THAT EMPLOYS ARTIFICIAL INTELLIGENCE BEFORE IMPLEMENTING THE SYSTEM;~~

(2) DEFINE THE CRITERIA FOR AN INVENTORY OF SYSTEMS THAT EMPLOY ~~RIGHTS IMPACTING OR SAFETY IMPACTING~~ HIGH-RISK ARTIFICIAL INTELLIGENCE;

~~(3) GOVERN THE PROCUREMENT, DEPLOYMENT, USE, AND ONGOING ASSESSMENT OF SYSTEMS THAT EMPLOY RIGHTS IMPACTING OR SAFETY IMPACTING ARTIFICIAL INTELLIGENCE FOR AN OPERATIONS RELATED PURPOSE BY A UNIT OF STATE GOVERNMENT IN PARTNERSHIP WITH A PUBLIC SENIOR HIGHER EDUCATION INSTITUTION OR WITH BALTIMORE CITY COMMUNITY COLLEGE;~~

(3) BE SUFFICIENT TO ENSURE THAT THE USE OF ANY SYSTEM THAT EMPLOYS ARTIFICIAL INTELLIGENCE BY A UNIT OF STATE GOVERNMENT IS GOVERNED BY ADEQUATE GUARDRAILS TO PROTECT INDIVIDUALS AND COMMUNITIES;

(4) IF THE DEPARTMENT IS NOTIFIED THAT AN INDIVIDUAL OR GROUP OF INDIVIDUALS MAY HAVE BEEN NEGATIVELY IMPACTED BY A SYSTEM THAT EMPLOYS HIGH-RISK ARTIFICIAL INTELLIGENCE, REQUIRE THE DEPARTMENT TO:

(I) NOTIFY AN INDIVIDUAL OR A GROUP OF INDIVIDUALS DETERMINED TO HAVE BEEN NEGATIVELY IMPACTED BY A SYSTEM THAT EMPLOYS RIGHTS IMPACTING OR SAFETY IMPACTING HIGH-RISK ARTIFICIAL INTELLIGENCE; AND

(II) PROVIDE GUIDANCE TO AN INDIVIDUAL OR A GROUP OF INDIVIDUALS DETERMINED TO HAVE BEEN NEGATIVELY IMPACTED BY A SYSTEM THAT EMPLOYS RIGHTS IMPACTING OR SAFETY IMPACTING HIGH-RISK ARTIFICIAL INTELLIGENCE ON AVAILABLE OPTIONS TO OPT OUT OF THE SYSTEM; AND

(5) PROVIDE GUIDANCE TO UNITS OF STATE GOVERNMENT ON PROCUREMENT OF A SYSTEM THAT EMPLOYS RIGHTS IMPACTING OR SAFETY IMPACTING HIGH-RISK ARTIFICIAL INTELLIGENCE THAT ENSURES DATA PRIVACY AND COMPLIANCE WITH APPLICABLE STATUTES AND REGULATIONS.

(C) THE DEPARTMENT SHALL MAKE THE POLICIES AND PROCEDURES REQUIRED BY SUBSECTION (A) OF THIS SECTION PUBLICLY AVAILABLE ON ITS WEBSITE WITHIN 45 DAYS AFTER THE POLICIES AND PROCEDURES ARE ADOPTED.

~~(D) EACH PUBLIC SENIOR HIGHER EDUCATION INSTITUTION AND BALTIMORE CITY COMMUNITY COLLEGE SHALL SUBMIT TO THE DEPARTMENT AN ANNUAL REPORT ON ARTIFICIAL INTELLIGENCE PROCURED AND DEPLOYED.~~

~~3.5-804. 3.5-805.~~

(A) BEGINNING ~~JULY~~ JANUARY JULY 1, 2025, A UNIT OF STATE GOVERNMENT MAY NOT PROCURE OR IMPLEMENT A DEPLOY A NEW SYSTEM THAT EMPLOYS ARTIFICIAL INTELLIGENCE UNLESS THE SYSTEM COMPLIES WITH THE POLICIES AND PROCEDURES ADOPTED UNDER § ~~3.5-803~~ 3.5-804 OF THIS SUBTITLE.

(B) A UNIT OF STATE GOVERNMENT THAT EMPLOYS RIGHTS IMPACTING OR SAFETY IMPACTING HIGH-RISK ARTIFICIAL INTELLIGENCE SHALL CONDUCT

REGULAR IMPACT ASSESSMENTS, AS DETERMINED BY THE GOVERNOR'S ARTIFICIAL INTELLIGENCE SUBCABINET OF THE GOVERNOR'S EXECUTIVE COUNCIL.

~~3.5-805.~~ **3.5-806.**

(A) THERE IS A GOVERNOR'S ARTIFICIAL INTELLIGENCE SUBCABINET OF THE GOVERNOR'S EXECUTIVE COUNCIL.

(B) THE PURPOSE OF THE SUBCABINET IS TO FACILITATE AND ENHANCE COOPERATION AMONG UNITS OF STATE GOVERNMENT, IN CONSULTATION WITH ACADEMIC INSTITUTIONS AND INDUSTRIES UTILIZING ARTIFICIAL INTELLIGENCE.

(C) THE SUBCABINET CONSISTS OF THE FOLLOWING MEMBERS:

(1) THE SECRETARY, OR THE SECRETARY'S DESIGNEE;

(2) THE SECRETARY OF BUDGET AND MANAGEMENT, OR THE SECRETARY'S DESIGNEE;

(3) THE SECRETARY OF GENERAL SERVICES, OR THE SECRETARY'S DESIGNEE;

(4) THE SECRETARY OF LABOR, OR THE SECRETARY'S DESIGNEE;

(5) THE SECRETARY OF COMMERCE, OR THE SECRETARY'S DESIGNEE;

(6) THE DIRECTOR OF THE GOVERNOR'S OFFICE OF HOMELAND SECURITY, OR THE DIRECTOR'S DESIGNEE;

(7) THE CHIEF PRIVACY OFFICER, OR THE CHIEF PRIVACY OFFICER'S DESIGNEE;

(8) THE CHIEF DATA OFFICER, OR THE CHIEF DATA OFFICER'S DESIGNEE;

(9) THE CHIEF INFORMATION SECURITY OFFICER, OR THE CHIEF INFORMATION SECURITY OFFICER'S DESIGNEE;

(10) THE GOVERNOR'S SENIOR ADVISOR FOR RESPONSIBLE ARTIFICIAL INTELLIGENCE, OR THE SENIOR ADVISOR'S DESIGNEE; AND

(11) ANY OTHER MEMBER OF THE GOVERNOR'S EXECUTIVE COUNCIL, APPOINTED BY THE GOVERNOR.

(D) THE SECRETARY SHALL CHAIR THE SUBCABINET.

(E) THE SUBCABINET SHALL:

(1) DEVELOP STRATEGY, POLICY, AND MONITORING PROCESSES FOR RESPONSIBLE AND PRODUCTIVE USE OF ARTIFICIAL INTELLIGENCE AND ASSOCIATED DATA BY UNITS OF STATE GOVERNMENT;

(2) OVERSEE THE STATE'S IMPLEMENTATION OF:

(I) ARTIFICIAL INTELLIGENCE INVENTORY;

(II) ~~DATA INVENTORY;~~

~~(III)~~ ARTIFICIAL INTELLIGENCE IMPACT ASSESSMENTS;

~~(IV) (III) MONITORING OF ARTIFICIAL INTELLIGENCE INVOLVING A HIGH-RISK ACTION RIGHTS IMPACTING OR SAFETY IMPACTING ARTIFICIAL INTELLIGENCE; AND~~

~~(III) MONITORING OF HIGH-RISK ARTIFICIAL INTELLIGENCE;~~
AND

~~(V) (IV)~~ COMPLIANCE WITH STATE POLICIES AND PROCEDURES;

(3) SUPPORT ARTIFICIAL INTELLIGENCE AND DATA INNOVATION ACROSS UNITS OF STATE GOVERNMENT ~~AND IN PRIVATE SECTOR ENTERPRISE BY;~~

~~(I) IDENTIFYING AND PRIORITIZING BEST USES OF ARTIFICIAL INTELLIGENCE IN EACH UNIT OF STATE GOVERNMENT AND IN PRIVATE SECTOR ENTERPRISE;~~

~~(II) TESTING PROOFS OF CONCEPT OF PRIORITY ARTIFICIAL INTELLIGENCE USE IN PROTOTYPING;~~

~~(III) REDUCING BARRIERS TO THE RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE AND STATE DATA;~~

~~(IV) DEVELOPING SUCCESSFUL ARTIFICIAL INTELLIGENCE PILOTS INTO PRODUCTION; AND~~

~~(V) TRAINING AND WORKFORCE DEVELOPMENT;~~

(4) DEVELOP AND IMPLEMENT A COMPREHENSIVE ACTION PLAN FOR RESPONSIBLE AND PRODUCTIVE USE OF ARTIFICIAL INTELLIGENCE AND ASSOCIATED DATA BY UNITS OF STATE GOVERNMENT;

(5) ESTABLISH PARTNERSHIPS, MEMORANDA OF UNDERSTANDING, AND CONTRACTS TO SUPPORT THE AIMS OF THIS SECTION;

(6) PROMOTE ARTIFICIAL INTELLIGENCE KNOWLEDGE, SKILLS, AND TALENT IN STATE GOVERNMENT ~~BY:~~

~~(I) IDENTIFYING AND OFFERING TRAINING PROGRAMS FOR STATE WORKERS ON THE USE OF ARTIFICIAL INTELLIGENCE AND PARTICULARLY GENERATIVE ARTIFICIAL INTELLIGENCE; AND~~

~~(II) EXPLORING WAYS TO PROVIDE EXTERNAL ARTIFICIAL INTELLIGENCE TALENT AN OPPORTUNITY TO SERVE THE STATE AND UNITS OF STATE GOVERNMENT IN TARGETED, SHORT TERM PROJECTS, INCLUDING BY LEVERAGING INSTITUTIONS OF HIGHER EDUCATION OR INDUSTRY; AND~~

(7) IDENTIFY ARTIFICIAL INTELLIGENCE USE CASES AND BUILD FOUNDATIONAL INFRASTRUCTURE BY REQUIRING:

(I) THE DEPARTMENT TO EVALUATE RELEVANT INFRASTRUCTURE TO SAFELY, SECURELY, AND EFFICIENTLY TEST ARTIFICIAL INTELLIGENCE PROOFS OF CONCEPT AND PILOTS;

(II) THE DEPARTMENT OF GENERAL SERVICES, IN CONSULTATION WITH THE DEPARTMENT, TO CREATE A MODEL FOR RUNNING AND PROCURING ARTIFICIAL INTELLIGENCE PROOFS OF CONCEPT AND PILOTS, IN ACCORDANCE WITH STATE LAWS, REGULATIONS, AND POLICIES; AND

(III) THE DEPARTMENT, IN CONSULTATION WITH THE SUBCABINET, TO COORDINATE WITH AGENCIES TO PROVIDE SUPPORT IN IDENTIFYING AND PRIORITIZING USE CASES AND EXECUTING PROOFS OF CONCEPT AND PILOTS ALIGNED WITH THE GOVERNOR'S PRIORITIES.

(F) THE GOVERNOR SHALL PROVIDE THE SUBCABINET WITH SUFFICIENT RESOURCES TO PERFORM THE FUNCTIONS OF THIS SECTION.

~~(G) FOR EACH FISCAL YEAR, THE GOVERNOR MAY INCLUDE IN THE ANNUAL BUDGET BILL AN APPROPRIATION OF UP TO \$3,000,000 FOR PARTNERSHIPS AND CONTRACTS TO SUPPORT THE FUNCTIONS REQUIRED IN THIS SECTION.~~

~~12-101.~~

~~(a) This section does not apply to:~~

~~(1) capital expenditures by the Department of Transportation or the Maryland Transportation Authority, in connection with State roads, bridges, or highways, as provided in § 12-202 of this title; [or]~~

~~(2) procurements by the Department of General Services AND THE DEPARTMENT OF INFORMATION TECHNOLOGY for the purpose of modernizing INFORMATION TECHNOLOGY AND cybersecurity infrastructure for the State valued below \$1,000,000; OR~~

~~(3) COMPETITIVE PROOF OF CONCEPT PROCUREMENTS VALUED BELOW \$1,000,000 MADE UNDER § 13-116 OF THIS ARTICLE.~~

~~(b) (1) The Board may control procurement by units.~~

~~(2) To implement the provisions of this Division II, the Board may:~~

~~(i) set policy;~~

~~(ii) adopt regulations, in accordance with Title 10, Subtitle 1 of the State Government Article; and~~

~~(iii) establish internal operational procedures consistent with this Division II.~~

~~(3) The Board shall ensure that the regulations of the primary procurement units provide for procedures that are consistent with this Division II and Title 13, Subtitle 4 of the State Personnel and Pensions Article and, to the extent the circumstances of a particular type of procurement or a particular unit do not require otherwise, are substantially the same.~~

~~(4) The Board may delegate any of its authority that it determines to be appropriate for delegation and may require prior Board approval for specified procurement actions.~~

~~(5) Except as limited by the Maryland Constitution, the Board may exercise any control authority conferred on a primary procurement unit by this Division II and, to the extent that its action conflicts with the action of the primary procurement unit, the action of the Board shall prevail.~~

~~(e) On or before December 1 each year, the Department of General Services shall submit a report to the Board on procurements made under subsection (a)(2) of this section that shall include for each procurement:~~

- ~~(1) the purpose of the procurement;~~
- ~~(2) the name of the contractor;~~
- ~~(3) the contract amount;~~
- ~~(4) the method of procurement utilized;~~
- ~~(5) the number of bidders who bid on the procurement; and~~
- ~~(6) the contract term.~~

~~(D) ON OR BEFORE DECEMBER 1 EACH YEAR, THE DEPARTMENT OF GENERAL SERVICES SHALL SUBMIT A REPORT TO THE BOARD ON PROCUREMENTS MADE UNDER SUBSECTION (A)(3) OF THIS SECTION THAT SHALL INCLUDE FOR EACH PROCUREMENT:~~

- ~~(1) THE PURPOSE OF THE PROCUREMENT;~~
 - ~~(2) THE NAME OF THE CONTRACTOR;~~
 - ~~(3) THE CONTRACT AMOUNT;~~
 - ~~(4) THE NUMBER OF PROPOSALS RECEIVED ON THE PROCUREMENT;~~
- AND**
- ~~(5) THE CONTRACT TERM.~~

13-116.

(A) IN THIS SECTION, “PROOF OF CONCEPT” MEANS A TEST, EVALUATION, DEMONSTRATION, OR PILOT PROJECT OF A ~~GOOD OR SERVICE~~ GOOD, SERVICE, OR TECHNOLOGY IN A REAL-WORLD ENVIRONMENT TO EVALUATE WHETHER THE ~~GOOD OR SERVICE~~ GOOD, SERVICE, OR TECHNOLOGY CAN BE SUCCESSFULLY DEPLOYED AND IS BENEFICIAL TO THE STATE.

(B) (1) A COMPETITIVE PROOF OF CONCEPT PROCUREMENT IS A FORMAL COMPETITIVE PROCUREMENT METHOD THAT MAY BE USED TO SOLICIT PROPOSALS FOR THE CONDUCT OF A PROOF OF CONCEPT PRIOR TO FULL IMPLEMENTATION WHEN THE HEAD OF A UNIT DETERMINES THE PROCESS TO BE APPROPRIATE AND IN THE BEST INTERESTS OF THE UNIT, INCLUDING:

(I) TESTING SOFTWARE-AS-A-SERVICE OR OFF-THE-SHELF SOFTWARE;

(II) TESTING NEW, INNOVATIVE PRODUCTS OR SERVICES; OR

(III) TESTING A PRODUCT OR SERVICE CONCEPTUALIZED OR CONCEIVED OF BY A UNIT OF STATE GOVERNMENT.

(2) (I) AFTER OBTAINING THE APPROVAL OF THE HEAD OF THE UNIT AND BEFORE CONDUCTING A COMPETITIVE PROOF OF CONCEPT PROCUREMENT, THE UNIT SHALL OBTAIN APPROVAL FROM THE SECRETARY OF INFORMATION TECHNOLOGY, OR THE SECRETARY'S DESIGNEE.

(II) THE SECRETARY OF INFORMATION TECHNOLOGY MAY GRANT APPROVAL FOR A COMPETITIVE PROOF OF CONCEPT PROCUREMENT IF THE UNIT:

1. HAS SUFFICIENT INTERNAL RESOURCES TO MANAGE THE PROOF OF CONCEPT, INCLUDING HUMAN CAPITAL, SUBJECT MATTER EXPERTISE, AND TECHNOLOGICAL INFRASTRUCTURE, OR HAS THE MEANS TO OBTAIN THESE RESOURCES; AND

2. ENTERS INTO A MEMORANDUM OF UNDERSTANDING WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY THAT REQUIRES REGULAR STATUS UPDATES, VENDOR CAPACITY, AND ANY OTHER INFORMATION NECESSARY FOR THE DEPARTMENT OF INFORMATION TECHNOLOGY TO EVALUATE WHETHER THE PROOF OF CONCEPT CAN BE SUCCESSFULLY DEPLOYED AND IS BENEFICIAL TO THE STATE.

(C) (1) A COMPETITIVE PROOF OF CONCEPT PROCUREMENT MAY BE CONDUCTED THROUGH THE ISSUANCE OF A SOLICITATION BY ANY METHOD OF PROCUREMENT AUTHORIZED UNDER THIS DIVISION II.

(2) A COMPETITIVE PROOF OF CONCEPT PROCUREMENT SOLICITATION SHALL INCLUDE A STATEMENT OF:

(I) THE SCOPE OF WORK OR PROJECT DESCRIPTION, INCLUDING THE INTENDED USE, QUANTITY, ESTIMATED TIME FRAME FOR THE PROOF OF CONCEPT, AND ANTICIPATED NUMBER OF PROOF OF CONCEPT AWARDS THAT WILL BE MADE; AND

(II) THE FACTORS, INCLUDING PRICE, THAT WILL BE USED IN EVALUATING PROPOSALS AND THE RELATIVE IMPORTANCE OF EACH.

(3) A SOLICITATION MAY BE DISTRIBUTED TO VENDORS KNOWN TO OFFER GOODS OR SERVICES WITHIN THE SCOPE OF THE PROOF OF CONCEPT AND SHALL, EXCEPT FOR PROCUREMENTS UNDER \$15,000 NOT OTHERWISE REQUIRED BY LAW TO BE POSTED, BE POSTED ON eMARYLAND MARKETPLACE ADVANTAGE, IN ACCORDANCE WITH THE POLICIES AND PROCEDURES UNDER SUBSECTION (G) OF THIS SECTION.

(D) AFTER RECEIPT OF PROPOSALS BUT BEFORE AWARD OF A PROCUREMENT CONTRACT, A UNIT MAY:

(1) CONDUCT DISCUSSIONS WITH AN OFFEROR TO ENSURE FULL UNDERSTANDING OF:

(I) THE REQUIREMENTS OF THE UNIT, AS SET FORTH IN THE REQUEST FOR PROPOSALS; AND

(II) THE PROPOSAL SUBMITTED BY THE OFFEROR; AND

(2) REQUEST PRODUCT SAMPLES FOR TESTING BY THE UNIT OR A DEMONSTRATION OF A PRODUCT OR SERVICE AND USE THESE SAMPLES OR DEMONSTRATIONS IN ITS EVALUATION PROCESS.

(E) A REQUEST FOR PRODUCT SAMPLES FOR TESTING OR DEMONSTRATION MADE UNDER SUBSECTION (D)(2) OF THIS SECTION SHALL BE ISSUED TO ALL OFFERORS DEEMED REASONABLE AT THE TIME OF THE REQUEST.

(F) A UNIT MAY:

~~(1) AWARD ONE OR MORE OF THE PROPOSALS A CONTRACT FOR THE PROOF OF CONCEPT; AND~~

~~(2) PROVIDE AN OPTION FOR THE STATE TO PROCEED WITH A FULL IMPLEMENTATION OF AN AWARDED PROPOSAL.~~

(G) A VENDOR AWARDED A PROOF OF CONCEPT PROCUREMENT SHALL BE ELIGIBLE TO BID ON A PROCUREMENT TO IMPLEMENT A PROPOSAL RELATED TO THE PROOF OF CONCEPT PROCUREMENT.

(H) THE DEPARTMENT OF GENERAL SERVICES, IN CONSULTATION WITH THE DEPARTMENT OF INFORMATION TECHNOLOGY, SHALL ADOPT POLICIES AND

**PROCEDURES FOR THE DEVELOPMENT AND IMPLEMENTATION OF COMPETITIVE
PROOF OF CONCEPT PROCUREMENTS.**

~~SECTION 2. AND BE IT FURTHER ENACTED, That, on or before December 1, 2024, the Governor's Artificial Intelligence Subcabinet of the Governor's Executive Council, in consultation with the appropriate stakeholders, shall submit an interim report and recommendations to the Governor and, in accordance with § 2-1257 of the State Government Article, the General Assembly on the risks and opportunities and associated recommendations related to:~~

~~(1) use of artificial intelligence to support job and business creation and growth in the State;~~

~~(2) in collaboration with the Maryland Department of Labor and, as appropriate, external experts, workers, labor unions, businesses, and civil society, use of artificial intelligence by the State workforce, including opportunities to upskill the workforce;~~

~~(3) in consultation with the Maryland Department of Emergency Management, the Public Service Commission, the Department of the Environment, and the Department of Transportation, use of artificial intelligence in critical infrastructure and guidelines for owners and operators to incorporate risk management into critical infrastructure, including mapping emergent cyber and physical security and resiliency risks to the State infrastructure and residents stemming from artificial intelligence;~~

~~(4) in consultation with the Maryland Department of Health, the U.S. Department of Veterans Affairs, and the U.S. Department of Homeland Security, use of systems that employ artificial intelligence in health care delivery and human services;~~

~~(5) in consultation with the Department of Information Technology Office of Security Management and the Chief Privacy Officer, use of artificial intelligence in the discovery and remediation of vulnerabilities in cybersecurity and data management across State and local government, including school systems;~~

~~(6) in consultation with the State Chief Privacy Officer and an independent contractor identified by the Subcabinet, data privacy, specifically regarding the potential to train systems that employ artificial intelligence;~~

~~(7) in consultation with the Maryland Department of Labor, the Department of Commerce, and the Governor's Office of Small, Minority, and Women Business Affairs, use of artificial intelligence in workforce training and hiring of talent with expertise in artificial intelligence, employment practices, and workforce development implications;~~

~~(8) in consultation with the Office of the Attorney General and the Judicial Branch, use of artificial intelligence in the criminal justice system, including whether and how such technology should be used, in what contexts, and with what safeguards;~~

~~(9) the procurement of systems that employ artificial intelligence, including efforts to increase competition and assurance that contracts retain sufficient data privacy protection against vendor lock in;~~

~~(10) use of artificial intelligence by occupations licensed and certified by the State, in consultation with the boards, identifying ways for the regulatory board to identify and manage the risks of opportunities of artificial intelligence and determine appropriate permitted use and supervision by licensees; and~~

~~(11) use of artificial intelligence in local school systems, including recommendations to the State on the responsible and productive use of artificial intelligence based on a review of the federal Department of Education Office of Educational Technology's report entitled "Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations", in collaboration with the State Department of Education.~~

SECTION 2. AND BE IT FURTHER ENACTED, That:

(a) The Governor's Artificial Intelligence Subcabinet of the Governor's Executive Council, in consultation with the appropriate units of State government, shall:

(1) develop a roadmap to review the risks and opportunities associated with the use of artificial intelligence in State services; and

(2) on or before December 1, 2024, submit the roadmap to the Governor and, in accordance with § 2-1257 of the State Government Article, the General Assembly.

(b) The roadmap developed under subsection (a) of this section shall include:

(1) a plan to study the use of artificial intelligence:

(i) to support job and business creation and growth in the State;

(ii) by the State workforce, including opportunities to upskill the workforce;

(iii) in critical infrastructure, including guidelines for owners and operators to incorporate risk management into critical infrastructure;

(iv) in health care delivery and human services;

(v) in the discovery and remediation of vulnerabilities in cybersecurity and data management across State and local government, including school systems;

(vi) in data privacy, specifically regarding the ability to train systems that employ artificial intelligence;

(vii) in workforce training;

(viii) in the criminal justice system and for public safety purposes, including whether and how such technology should be used, in what contexts, and with what safeguards;

(ix) by occupations licensed and certified by the State, including identifying ways for State regulatory boards to identify and manage the risks and opportunities of artificial intelligence and determine appropriate permitted use and supervision of licensees;

(x) in local school systems, including recommendations to the State on the responsible and productive use of artificial intelligence;

(xi) in the conduct of elections, including reducing or eliminating the spread of misinformation; and

(xii) any other State service identified by the Subcabinet;

(2) a plan to study:

(i) the hiring of talent with expertise in artificial intelligence, employment practices, and workforce development implications;

(ii) methods to ensure that there is diversity in contract awards and training programs related to artificial intelligence in the State, including racial diversity; and

(iii) the procurement of systems that employ artificial intelligence, including efforts to increase competition and assurance that contracts retain sufficient data privacy protection against vendor lock-in;

(3) a prioritization of the study topics listed under this subsection, including the methodology for the prioritization;

(4) a list of appropriate stakeholders identified to participate in each study topic; and

(5) the projected timeline to complete each study topic.

SECTION 3. AND BE IT FURTHER ENACTED, That, on or before December 1, 2025, the Governor's Artificial Intelligence Subcabinet of the Governor's Executive Council shall submit a report and recommendations to the Governor and, in accordance with § 2-1257 of the State Government Article, the General Assembly on the sufficiency of the Subcabinet to accomplish the artificial intelligence goals of the State and the efficacy of the potential transition of the Subcabinet to a department or independent unit of State government.

~~SECTION 4. AND BE IT FURTHER ENACTED, That it is the intent of the General Assembly that the Department of Information Technology:~~

~~(1) evaluate the potential of artificial intelligence in creating a statewide virtual 3-1-1 portal as a source for Maryland residents to obtain nonemergency government information and services; and~~

~~(2) if the Department determines that the use of artificial intelligence in creating a virtual 3-1-1 portal is feasible, to prioritize the creation of a virtual 3-1-1 portal through a competitive proof of concept procurement in accordance with § 13-116 of the State Finance and Procurement Article, as enacted by Section 1 of this Act.~~

SECTION 4. AND BE IT FURTHER ENACTED, That it is the intent of the Maryland General Assembly, contingent on the passage of S.B. 955 or H.B. 1174 of the Acts of the General Assembly of 2024 by both Houses of the General Assembly, that the Governor's Artificial Intelligence Subcabinet consult with the Technology Advisory Commission established under S.B. 955 or H.B. 1174 of the Acts of the General Assembly of 2024 in the performance of its duties under Sections 1 and 2 of this Act.

SECTION ~~4~~ 5. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2024.

Approved by the Governor, May 9, 2024.

Dutch scandal serves as a warning for Europe over

Uploaded by: Katie Fry Hester

Position: FAV

NEWS TECHNOLOGY

Dutch scandal serves as a warning for Europe over risks of using algorithms

The Dutch tax authority ruined thousands of lives after using an algorithm to spot suspected benefits fraud — and critics say there is little stopping it from happening again.

 SHARE

POLITICO

Free article usually reserved for subscribers



As the world turns to AI to automate their systems, the Dutch scandal shows how devastating they can be | Dean Mouhtaropoulos/Getty Images

MARCH 29, 2022 6:14 PM CET
BY MELISSA HEIKKILÄ

Chermaine Leysner's life changed in 2012, when she received a letter from the Dutch tax authority demanding she pay back her child care allowance going back to 2008. Leysner, then a student studying social work, had three children under the age of 6. The tax bill was over €100,000.

"I thought, 'Don't worry, this is a big mistake.' But it wasn't a mistake. It was the start of something big," she said.

The ordeal took nine years of Leysner's life. The stress caused by the tax bill and her mother's cancer diagnosis drove Leysner into depression and burnout. She ended up separating from her children's father. "I was working like crazy so I could still do something for my children like give them some nice things to eat or buy candy. But I had times that my little boy had to go to school with a hole in his shoe," Leysner said.

Advertisement

Leysner is one of the tens of thousands of victims of what the Dutch have dubbed the “*toeslagenaffaire*,” or the child care benefits scandal.

In 2019 it was revealed that the Dutch tax authorities had used a self-learning algorithm to create risk profiles in an effort to spot child care benefits fraud.

Authorities penalized families over a mere suspicion of fraud based on the system’s risk indicators. Tens of thousands of families — often with lower incomes or belonging to ethnic minorities — were pushed into poverty because of exorbitant debts to the tax agency. Some victims committed suicide. More than a thousand children were taken into foster care.

The Dutch tax authorities now face a new €3.7 million fine from the country's privacy regulator. In a statement released April 12, the agency outlined several violations of the EU's data protection rulebook, the General Data Protection Regulation, including not having a legal basis to process people's data and hanging on to the information for too long.

Aleid Wolfsen, the head of the Dutch privacy authority, called the violations unprecedented.

"For over 6 years, people were often wrongly labeled as fraudsters, with dire consequences ... some did not receive a payment arrangement or you were not eligible for debt restructuring. The tax authorities have turned lives upside down," he said, according to the statement.

Advertisement

Advertisement

As governments around the world are turning to algorithms and AI to automate their systems, the Dutch scandal shows just how utterly devastating automated systems can be without the right safeguards. The European Union, which positions itself as the world's leading tech regulator, is working on a bill that aims to curb algorithmic harms.

But critics say the bill misses the mark and would fail to protect citizens from incidents such as what happened in the Netherlands.

No checks and balances

The Dutch system — which was launched in 2013 — was intended to weed out benefits fraud at an early stage. The criteria for the risk profile were developed by the tax authority, reports Dutch newspaper Trouw. Having dual nationality was marked as a big risk indicator, as was a low income.

Why Leysner ended up in the situation is unclear. One reason could be that she had twins, which meant she needed more support from the government. Leysner, who was born in the Netherlands, also has Surinamese roots.

In 2020, Trouw and another Dutch news outlet, RTL Nieuws revealed that the tax authorities also kept secret blacklists of people for two decades, which tracked both credible and unsubstantiated “signals” of potential fraud. Citizens had no way of finding out why they were on the list or defending themselves.

An audit showed that the tax authorities focused on people with “a non-Western appearance,” while having Turkish or Moroccan nationality was a particular focus. Being on the blacklist also led to a higher risk score in the child care benefits system.

Advertisement

A parliamentary report into the child care benefits scandal found several grave shortcomings, including institutional biases and authorities hiding information or misleading the parliament about the facts. Once the full scale of the scandal came to light, Prime Minister Mark Rutte's government resigned, only to regroup 225 days later.

In addition to the penalty announced April 12, the Dutch data protection agency also fined the Dutch tax administration €2.75 million in December 2021 for the “unlawful, discriminatory and therefore improper manner” in which the tax authority processed data on the dual nationality of child care benefit applicants.

“There was a total lack of checks and balances within every organization of making sure people realize what was going on,” said Pieter Omtzigt, an independent member of the Dutch parliament who played a pivotal role in uncovering the scandal and grilling the tax authorities.

“What is really worrying me is that I’m not sure that we’ve taken even vaguely enough preventive measures to strengthen our institutions to handle the next derailment,” he continued.

The new Rutte government has pledged to create a new algorithm regulator under the country’s data protection authority. Dutch Digital Minister Alexandra van Huffelen — who was previously the finance minister in charge of the tax authority — told POLITICO that the data authority’s role will be “to oversee the creation of algorithms and AI, but also how it plays out when it’s there, how it’s treated, make sure that is human-centered, and that it does apply to all the regulations that are in use.” The regulator will scrutinize algorithms in both the public and private sectors.

Van Huffelen stressed the need to make sure humans are always in the loop. “What I find very important is to make sure that decisions, governmental decisions based on AI are also always treated afterwards by a human person,” she said.

Advertisement

Advertisement

A warning to the rest of Europe

Europe's top digital official, European Commission Executive Vice President Margrethe Vestager, said the Dutch scandal is exactly what every government should be scared of.

“We have huge public sectors in Europe. There are so many different services where decision-making supported by AI could be really useful, if you trust it,” Vestager told the European Parliament in March. The EU's new AI Act is aimed at creating that trust, she argued, “so that this big public sector market will be open also for artificial intelligence.”

The Commission's proposal for the AI Act restricts the use of so-called high-risk AI systems and bans certain “unacceptable” uses. Companies providing high-risk AI systems have to meet certain EU requirements. The AI Act also creates a public EU register of such systems in an effort to improve transparency and help with enforcement.

That's not good enough, argues Renske Leijten, a Socialist member of the Dutch parliament and another key politician who helped uncover the true scale of the scandal. Leijten argues that the AI Act should also apply to those using high-risk AI systems in both the private and public sectors.

In the AI Act, “we see that there are more guarantees for your rights when companies and private enterprises are working with AI. But the important thing we must learn out of the child care benefit scandal is that this was not an enterprise or private sector ... This was the government,” she said.

As it is now, the AI Act will not protect citizens from similar dangers, said Dutch Green MEP Kim van Sparrentak, a member of the European Parliament’s AI Act negotiating team on the internal market committee. Van Sparrentak is pushing for the AI Act to have fundamental rights impact assessments that will also be published in the EU’s AI register. Parliament is also proposing adding obligations to the users of high-risk AI systems, including in the public sector.

Advertisement

Advertisement

“Fraud prediction and predictive policing based on profiling should just be banned. Because we have seen only very bad outcomes and not a single person can be determined based on some of their data,” van Sparrentak said.

In a report detailing how the Dutch government used ethnic profiling in the child care benefits scandal, Amnesty International calls on governments to ban the “use of data on nationality and ethnicity when risk-scoring for law enforcement purposes in the search of potential crime or fraud suspects.”

The Netherlands is still reckoning with the aftermath of the scandal. The government has promised to pay back victims of the incident €30,000. But for those like Leysner, that doesn't even begin to cover the years she lost — justice seems like a long way off.

“If you go through things like this, you also lose your trust in the government. So it's very difficult to trust what [authorities] say right now,” Leysner said.

Clothilde Goujard and Vincent Manancourt contributed reporting.

This article has been updated with the results of the Dutch tax authorities' investigation released in April.

Advertisement

[Algorithms](#)[Artificial Intelligence](#)[Data](#)[Data protection](#)[Fraud](#)[Law enforcement](#)[Policing](#)[Rights](#)[Services](#)[Tax](#)[Transparency](#)

🌐 Related Countries

[The Netherlands](#)

👤 Related People

[Kim van Sparrentak](#)[Margrethe Vestager](#)

🏢 Related Organizations

[European Commission](#)[European Parliament](#)

○ Our readers read next



Ukraine and US agree to minerals deal, reports say

59 MINS AGO 2 MINS READ



Trump's defense deputy secretary pick avoids saying Russia invaded Ukraine

2 HRS AGO 4 MINS READ



UK hikes defense spending to 2.5 percent by cutting aid

7 HRS AGO 5 MINS READ



Macron to Trump: Make trade war with China, not with us

9 HRS AGO 2 MINS READ

[More from Melissa Heikkilä](#)



Putin's aggression pushes Nordics closer to NATO than ever

Finnish President Sauli Niinistö will meet US President Joe Biden to discuss the war in Europe.

MAR 4 3 MINS READ



Finnish lawmakers to discuss potential NATO membership

Prime Minister Sanna Marin also announced that Finland would provide Ukraine with lethal aid.

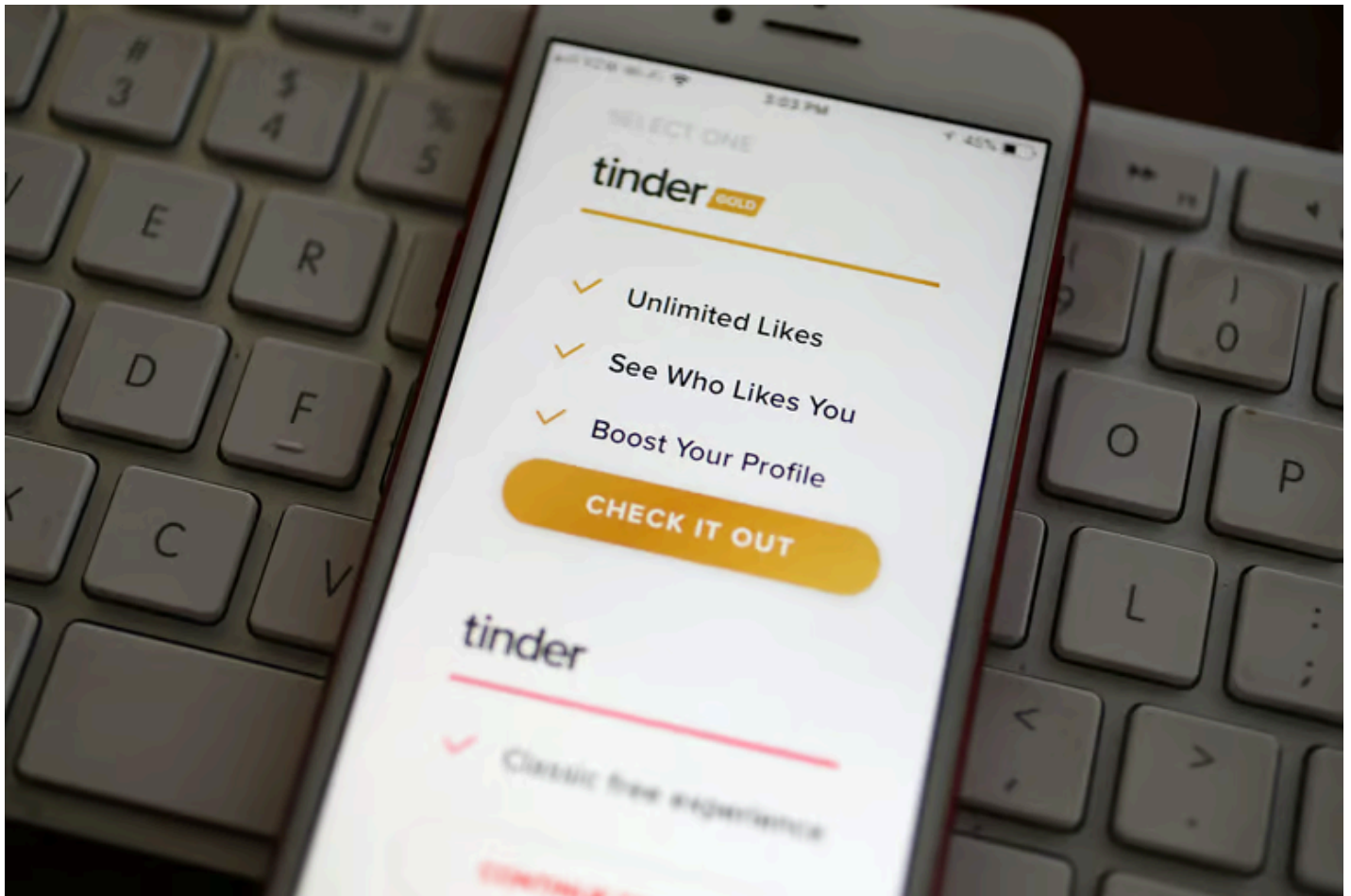
FEB 28 2 MINS READ



UN fired tech envoy after probe showed ‘pattern’ of harassment, documents show

International organization had already been searching for a replacement.

JAN 26 4 MINS READ



UK consumer group: Tinder's pricing algorithm discriminates against over-30s

Which? accuses the popular dating app of breaking data protection law.

JAN 21 3 MINS READ

POLITICO

POLICY

Agriculture and Food

Competition and Industrial Policy

Defense

Energy and Climate UK

Financial Services

Central Banker

Cybersecurity and Data Protection

Energy and Climate

Energie et Climat France

Financial Services UK

Health Care
Paris Influence
Technology
Technology UK
Trade UK

Mobility
Sustainability
Tech France
Trade

NEWSLETTERS

Berlin Bulletin
Brussels Playbook
Dimanchissime
EU Influence
Global Policy Lab: Living Cities
London Playbook
POLITICO Confidential

Berlin Playbook
China Watcher
EU Election Playbook
Global Playbook
London Influence
Playbook Paris
Sunday Crunch

PODCASTS

EU Confidential
Power Play
Berlin Playbook — Der Podcast

Politics at Jack and Sam's
Westminster Insider

OPINION

All Opinion
Club Med
From Across the Pond

Beyond the Bubble
Declassified
Unpacked

FEATURED SERIES

Polish Presidency of the EU
Living Cities

A global emergency: Tackling antimicrobial resistance
POLITICO 28

SUBSCRIPTIONS

POLITICO Pro
Research and analysis division

Print Edition

Michigan's MiDAS Unemployment System_ Algorithm AI

Uploaded by: Katie Fry Hester

Position: FAV

NEWS COMPUTING

Michigan's MiDAS Unemployment System: Algorithm Alchemy Created Lead, Not Gold > A case study into how to automate false accusations of fraud for more than 34,000 unemployed people

BY ROBERT N. CHARETTE

24 JAN 2018

Robert N. Charette is a Contributing Editor and an acknowledged international authority on information technology and systems risk management.

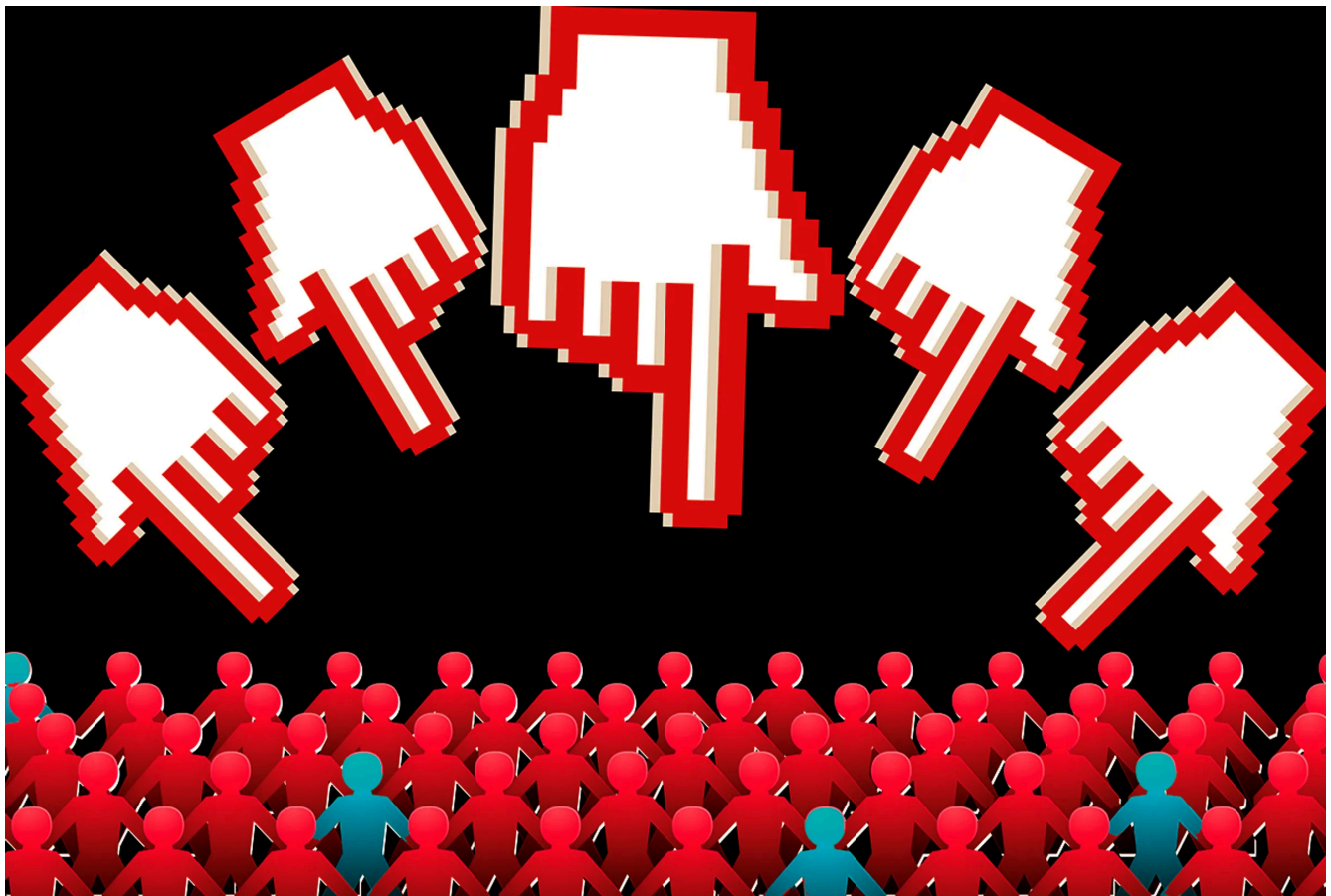




ILLUSTRATION: ISTOCKPHOTO/IEEE SPECTRUM

PERHAPS NEXT MONTH, THOSE 34,000-PLUS individuals wrongfully accused of unemployment fraud in Michigan from October 2013 to September 2015 will finally hear that they will receive some well-deserved remuneration for the harsh treatment meted out by Michigan Integrated Data Automated System (MiDAS). Michigan legislators have promised to seek at least US \$30 million in compensation for those falsely accused.

This is miserly, given how many people experienced punishing personal trauma, hired lawyers to defend themselves, saw their credit and reputations ruined, filed for bankruptcy, had their houses foreclosed, or were made homeless. A sum closer to \$100 million, as some are advocating, is probably warranted.

The fiasco is all too familiar: A government agency wants to replace a legacy IT system to gain cost and operational efficiencies, but alas, the effort goes horribly wrong because of gross risk mismanagement.

This time, it was the Michigan Unemployment Insurance Agency (UIA) which wanted to replace a 30-year-old mainframe system running COBOL. The objectives of the new system were threefold and reasonable. First, ensure that unemployment checks were going only to people who deserved them. Second, increase UIA's efficiency and responsiveness to unemployment claims. And third, through those efficiency gains, reduce UIA's operational costs by eliminating more than 400 workers, or about one-third of the agency's staff. After spending \$44,400,558 and 26 months on the effort, the UIA launched MiDAS, and soon proclaimed it a huge success [PDF], coming in under budget and on time, and discovering previously missed fraudulent unemployment filings.

Finding Fake Fraud

Soon after MiDAS was put into operation, the number of persons suspected of unemployment fraud grew fivefold in comparison to the average number found using the old system [PDF]. The newfound fraud and the fines imposed generated huge amounts of money for the UIA, increasing its coffers from around \$3 million to more than \$69 million in a little more than a year.



A review found that MiDAS adjudicated—by algorithm alone—40,195 cases of fraud, with 85 percent resulting in incorrect fraud determinations

The cash windfall was due in part to the harsh penalties imposed on those accused, such as the levy of a 400 percent penalty on the claimed amount of fraud [PDF], the highest in the nation.

Further, once a claim was substantiated, the state could immediately go after a person's wages and federal and state income tax refunds, and make a criminal referral if payments weren't forthcoming.

While the UIA was patting itself on the back for a job well done, unemployment lawyers and advocates noticed a huge spike in appeals by those accused of fraud. In instance after instance, the accusations of fraud were subsequently thrown out on appeal. Digging deeper, the lawyers and advocates discovered [PDF] that a large number of fraud accusations were being generated algorithmically by MiDAS, with no human intervention or review of the accusation possible, as

required with the legacy system.

In addition, the MiDAS-generated notices of fraud that claimants had to respond to were designed in such a way as to almost ensure someone inadvertently would admit to fraud. MiDAS also accused some people of fraud even though they had never received any unemployment. Furthermore, MiDAS was apparently basing some of its findings on missing or corrupt data. In effect, MiDAS was built upon the assumption that anyone claiming unemployment insurance was trying to defraud the UIA, and it was up to claimants to prove otherwise.

All the failings of MiDAS are too numerous to repeat here; I suggest you read the many excellent published stories such as these ([here](#) and [here](#)) from the *Detroit MetroTimes* and [here](#) from the Center of Michigan for more details and links to other articles which will leave you shaking your head in disbelief at the callousness shown by the UIA.

What's also inexcusable is that, though 64 percent of fraud claims were in the process of being reviewed or overturned on appeals in administrative court, the UIA stubbornly defended MiDAS (and all the "surplus money" it was generating to cover state spending) against internal warnings that

something was wrong with the MiDAS fraud determination

something was wrong with now MiDAS was determining fraud. However, the public and political outcry finally forced the UIA to admit that perhaps there was indeed a significant problem with MiDAS, especially its “robo-adjudication” process and the lack of human review. The UIA decided to cease using MiDAS for purely automated fraud assessment in September 2015, after pressure from the federal government and the filing of a federal lawsuit against the agency that same month.

The federal lawsuit against the state concluded in January 2017 with the UIA finally apologizing for the false claims of unemployment fraud. A thorough review found that from October 2013 to September 2015, MiDAS adjudicated—by algorithm alone—40,195 cases of fraud, with 85 percent of those resulting in incorrect fraud determinations. Another 22,589 cases that had some level of human interaction involved in a fraud determination found a 44 percent false fraud claim rate, which was an “improvement” but still an incredibly poor result. Interestingly, but not surprisingly, the UIA has stubbornly refused to explain exactly why MiDAS failed so spectacularly, or why it ignored all the early warning signs that something was radically amiss.

While the UIA says it sympathizes with those it falsely

accused of fraud, and has supposedly returned all the fines it had collected, the UIA has also strenuously fought against the class-action lawsuit [PDF] brought against it for the personal and financial damages those phony accusations created. The UIA strongly lauded a state appellate court ruling in July 2017 dismissing the lawsuit because those wrongly accused missed the deadline for making their compensation claims.

Given that the UIA stonewalled all attempts to discover the depth, breadth, and reasons behind the fraudulent fraud accusations, the ruling may be legally correct, but it is morally ludicrous. The ruling, which is being appealed to Michigan's Supreme Court, so shamed the state's legislators and governor that they agreed to changes to the state's unemployment law and, at least, in principle, to the creation of a MiDAS victim compensation fund. We'll see next month whether one actually is created.

Michigan Is Not Alone

The MiDAS fiasco is not the only case where robo-adjudication has been used to seek potential benefits fraud. It is alive and well in Australia, where the government's Centrelink program rolled out a similar approach in 2016 with similar results. Tens of thousands of benefit recipients have

received letters from Centrelink stating that they have to prove that they haven't applied for benefits they didn't deserve, with more than 20 percent receiving the notices in error or with debt amounts significantly in excess of what they actually owed. The Australian government has insisted from the start that the automated system Centrelink is working as intended, which according to at least one report, works poorly by design as a way to cut operational costs, if not generate money it isn't legally owed. When a parliamentary group recommended that the robo-adjudication process be halted, the government refused to hear of it.



As algorithms take on more decisions, it is imperative that those affected can understand and challenge how these decisions are being made

In a thoughtful paper by California Supreme Court Justice Mariano-Florentino Cuéllar called “Cyberdelegation and the Administrative State,” he points out that a real problem with bureaucratic decisions made purely by algorithm is the hesitancy of the human overseers to question the results generated by the algorithm. Justice Cuéllar cites the case of

the U.S. Veteran's Administration's implementation of an automated disability rating system to reduce paperwork and personnel costs and increase productivity that significantly overestimated the disability benefits veterans should have received in comparison to what a human rater would have approved. In fact, in 1.4 million algorithmically made rating assessments, only 2 percent were later overridden. The same hesitancy to see anything wrong with automated decisions occurred with both MiDAS and Centrelink.

As algorithms take on even more decisions [PDF] in the criminal justice system, in corporate and government hiring, in approving credit and the like, it is imperative that those affected can understand and challenge how these decisions are being made. Hopefully, the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems will help ensure that the risks of automated decision-making systems are not glossed over in the quest for their benefits, which potentially can be immense. I don't think any of us would want to end up in the same type of nightmare robo-adjudication process as those in the MiDAS situation sadly

did

This article is for IEEE members only. Join IEEE to access our full archive.

Join the world's largest professional organization devoted to engineering and applied sciences and get access to all of Spectrum's articles, podcasts, and special reports. [Learn more →](#)

If you're already an IEEE member, please sign in to continue reading.

BECOME A MEMBER

SIGN IN

OMB Memo.pdf

Uploaded by: Katie Fry Hester

Position: FAV




EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

March 28, 2024

M-24-10

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young 

SUBJECT: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence

Artificial intelligence (AI) is one of the most powerful technologies of our time, and the President has been clear that we must seize the opportunities AI presents while managing its risks. Consistent with the AI in Government Act of 2020,¹ the Advancing American AI Act,² and Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, this memorandum directs agencies to advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public.³

1. OVERVIEW

While AI is improving operations and service delivery across the Federal Government, agencies must effectively manage its use. As such, this memorandum establishes new agency requirements and guidance for AI governance, innovation, and risk management, including through specific minimum risk management practices for uses of AI that impact the rights and safety of the public.

Strengthening AI Governance. Managing AI risk and promoting AI innovation requires effective AI governance. As required by Executive Order 14110, each agency must designate a Chief AI Officer (CAIO) within 60 days of the date of the issuance of this memorandum. This memorandum describes the roles, responsibilities, seniority, position, and reporting structures for agency CAIOs, including expanded reporting through agency AI use case inventories. Because AI is deeply interconnected with other technical and policy areas including data, information technology (IT), security, privacy, civil rights and civil liberties, customer experience, and

¹ Pub. L. No. 116-260, div. U, title 1, § 104 (codified at 40 U.S.C. § 11301 note), <https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf>.

² Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301 note), <https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>.

³ This memorandum accounts for public comments that OMB received following its publication of a draft version of this memorandum on November 1, 2023. OMB has separately published an explanation and response to public comments, available at <https://www.regulations.gov/document/OMB-2023-0020-0001>.

workforce management, CAIOs must work in close coordination with existing responsible officials and organizations within their agencies.

Advancing Responsible AI Innovation. With appropriate safeguards in place, AI can be a helpful tool for modernizing agency operations and improving Federal Government service to the public. To that end, agencies must increase their capacity to responsibly adopt AI, including generative AI, and take steps to enable sharing and reuse of AI models, code, and data. This memorandum requires each agency identified in the Chief Financial Officers Act (CFO Act)⁴ to develop an enterprise strategy for how they will advance the responsible use of AI. This memorandum also provides recommendations for how agencies should reduce barriers to the responsible use of AI, including barriers related to IT infrastructure, data, cybersecurity, workforce, and the particular challenges of generative AI.

Managing Risks from the Use of AI. While agencies will realize significant benefits from AI, they must also manage a range of risks from the use of AI. Agencies are subject to existing risk management requirements relevant to AI, and this memorandum does not replace or supersede these requirements. Instead, it establishes new requirements and recommendations that, both independently and collectively, address the specific risks from relying on AI to inform or carry out agency decisions and actions, particularly when such reliance impacts the rights and safety of the public. To address these risks, this memorandum requires agencies to follow minimum practices when using safety-impacting AI and rights-impacting AI, and enumerates specific categories of AI that are presumed to impact rights and safety. Finally, this memorandum also establishes a series of recommendations for managing AI risks in the context of Federal procurement.⁵

2. SCOPE

Agency adoption of AI poses many challenges, some novel and specific to AI and some well-known. While agencies must give due attention to all aspects of AI, this memorandum is more narrowly scoped to address a subset of AI risks, as well as governance and innovation issues that are directly tied to agencies' use of AI. The risks addressed in this memorandum result from any reliance on AI outputs to inform, influence, decide, or execute agency decisions or actions, which could undermine the efficacy, safety, equitableness, fairness, transparency, accountability, appropriateness, or lawfulness of such decisions or actions.⁶

⁴ 31 U.S.C. § 901(b).

⁵ Consistent with provisions of the AI in Government Act of 2020, the Advancing American AI Act, and Executive Order 14110 directing the publication of this memorandum, this memorandum sets forth multiple independent requirements and recommendations for agencies, and OMB intends that these requirements and recommendations be treated as severable. For example, the memorandum's provisions regarding the strengthening of AI governance in Section 2 are capable of operating independently, and serve an independent purpose, from the required risk management practices set forth in Section 5. Likewise, each of Section 5's individual risk management practices serves an independent purpose and can function independently from the other risk management practices. Accordingly, while this memorandum governs only agencies' own use of AI and does not create rights or obligations for the public, in the event that a court were to stay or enjoin application of a particular provision of this memorandum, or its application to a particular factual circumstance, OMB would intend that the remainder of the memorandum remain operative.

⁶ The subset of AI risks addressed in this memorandum is generally referred to in this document as "risks from the use of AI", and a full definition for this term is provided in Section 6.

This memorandum does not address issues that are present regardless of whether AI is used versus any other software, such as issues with respect to Federal information and information systems in general. In addition, this memorandum does not supersede other, more general Federal policies that apply to AI but are not focused specifically on AI, such as policies that relate to enterprise risk management, information resources management, privacy, accessibility, Federal statistical activities, IT, or cybersecurity.

Agencies must continue to comply with applicable OMB policies in other domains relevant to AI, and to coordinate compliance across the agency with all appropriate officials. All agency responsible officials retain their existing authorities and responsibilities established in other laws and policies.

a. Covered Agencies. Except as specifically noted, this memorandum applies to all agencies defined in 44 U.S.C. § 3502(1).⁷ As noted in the relevant sections, some requirements in this memorandum apply only to Chief Financial Officers Act (CFO Act) agencies as identified in 31 U.S.C. § 901(b), and other requirements do not apply to elements of the Intelligence Community, as defined in 50 U.S.C. § 3003.

b. Covered AI. This memorandum provides requirements and recommendations that, as described in more detail below, apply to new and existing AI that is developed, used, or procured by or on behalf of covered agencies. This memorandum does not, by contrast, govern:

- i. agencies' regulatory actions designed to prescribe law or policy regarding non-agency uses of AI;
- ii. agencies' evaluations of particular AI applications because the AI provider is the target or potential target of a regulatory enforcement, law enforcement, or national security action;⁸
- iii. agencies' development of metrics, methods, and standards to test and measure AI, where such metrics, methods, and standards are for use by the general public or the government as a whole, rather than to test AI for a particular agency application⁹; or
- iv. agencies' use of AI to carry out basic research or applied research, except where the purpose of such research is to develop particular AI applications within the agency.

⁷ The term "agency," as used in both the AI in Government Act of 2020 and the Advancing American AI Act, is defined as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency," but does not include the Government Accountability Office; the Federal Election Commission; the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities. 44 U.S.C. § 3502(1); *see* AI in Government Act of 2020 § 102(2) (defining "agency" by reference to § 3502); Advancing American AI Act § 7223(1) (same). As a result, independent regulatory agencies as defined in 44 U.S.C. § 3502(5), which were not included in the definitions of "agency" in Executive Order 13960 and Executive Order 14110, *are* covered by this memorandum.

⁸ AI is not in scope when it is the target or potential target of such an action, but it is in scope when the AI is used to *carry out* an enforcement or national security action. For example, when evaluating an AI tool to determine whether it violates the law, the AI would not be in scope; if agencies were using that same tool to assess a different target, then the AI would be in scope.

⁹ Examples include agency actions to develop, for general use, standards or testing methodologies for evaluating or red-teaming AI capabilities.

The requirements and recommendations of this memorandum apply to system functionality that implements or is reliant on AI, rather than to the entirety of an information system that incorporates AI. As noted in the relevant sections, some requirements in this memorandum apply only in specific circumstances in which agencies use AI, such as when the AI may impact rights or safety.

c. Applicability to National Security Systems. This memorandum does not cover AI when it is being used as a component of a National Security System.¹⁰

3. STRENGTHENING ARTIFICIAL INTELLIGENCE GOVERNANCE

The head of each covered agency is responsible for pursuing AI innovation and ensuring that their agency complies with AI requirements in relevant law and policy, including the requirement that risks from the agency's use of AI are adequately managed. Doing so requires a strong governance structure and agencies are encouraged to strategically draw upon their policy, programmatic, research and evaluation, and regulatory functions to support the implementation of this memorandum's requirements and recommendations. The head of each covered agency must also consider the financial, human, information, and infrastructure resources necessary for implementation, prioritizing current resources or requesting additional resources via the budget process, as needed to support the responsibilities identified in this memorandum.

To improve accountability for AI issues, agencies must designate a Chief AI Officer, consistent with Section 10.1(b) of Executive Order 14110. CAIOs bear primary responsibility on behalf of the head of their agency for implementing this memorandum and coordinating implementation with other agencies. This section defines CAIOs' roles, responsibilities, seniority, position, and reporting structure.

a. Actions

- i. **Designating Chief AI Officers.** Within 60 days of the issuance of this memorandum, the head of each agency must designate a CAIO. To ensure the CAIO can fulfill the responsibilities laid out in this memorandum, agencies that have already designated a CAIO must evaluate whether they need to provide that individual with additional authority or appoint a new CAIO. Agencies must identify these officers to OMB through OMB's Integrated Data Collection process or an OMB-designated successor process. When the designated individual changes or the position is vacant, agencies must notify OMB within 30 days.
- ii. **Convening Agency AI Governance Bodies.** Within 60 days of the issuance of this memorandum, each CFO Act agency must convene its relevant senior officials to

¹⁰ AI innovation and risk for National Security Systems must be managed appropriately, but these systems are governed through other policy. For example, Section 4.8 of Executive Order 14110 directs the development of a National Security Memorandum to govern the use of AI as a component of a National Security System, and agencies also have existing guidelines in place, such as the Department of Defense's (DoD) *Responsible Artificial Intelligence Strategy and Implementation Pathway* and the Office of the Director of National Intelligence's *Principles of Artificial Intelligence Ethics for the Intelligence Community*, as well as policies governing specific high-risk national security applications of AI, such as DoD Directive 3000.09, *Autonomy in Weapon Systems*.

coordinate and govern issues tied to the use of AI within the Federal Government, consistent with Section 10.1(b) of Executive Order 14110 and the detailed guidance in Section 3(c) of this memorandum.

- iii. **Compliance Plans.** Consistent with Section 104(c) and (d) of the AI in Government Act of 2020, within 180 days of the issuance of this memorandum or any update to this memorandum, and every two years thereafter until 2036, each agency must submit to OMB and post publicly on the agency’s website either a plan to achieve consistency with this memorandum, or a written determination that the agency does not use and does not anticipate using covered AI. Agencies must also include plans to update any existing internal AI principles and guidelines to ensure consistency with this memorandum.¹¹ OMB will provide templates for these compliance plans.
- iv. **AI Use Case Inventories.** Each agency (except for the Department of Defense and the Intelligence Community) must individually inventory each of its AI use cases at least annually, submit the inventory to OMB, and post a public version on the agency’s website. OMB will issue detailed instructions for the inventory and its scope through its Integrated Data Collection process or an OMB-designated successor process. Beginning with the use case inventory for 2024, agencies will be required, as applicable, to identify which use cases are safety-impacting and rights-impacting AI and report additional detail on the risks—including risks of inequitable outcomes—that such uses pose and how agencies are managing those risks.
- v. **Reporting on AI Use Cases Not Subject to Inventory.** Some AI use cases are not required to be individually inventoried, such as those in the Department of Defense or those whose sharing would be inconsistent with applicable law and governmentwide policy. On an annual basis, agencies must still report and release aggregate metrics about such use cases that are otherwise within the scope of this memorandum, the number of such cases that impact rights and safety, and their compliance with the practices of Section 5(c) of this memorandum. OMB will issue detailed instructions for this reporting through its Integrated Data Collection process or an OMB-designated successor process.

b. Roles, Responsibilities, Seniority, Position, and Reporting Structure of Chief Artificial Intelligence Officers

Consistent with Section 10.1(b)(ii) of Executive Order 14110, this memorandum defines CAIOs’ roles, responsibilities, seniority, position, and reporting structures as follows:

- i. **Roles.** CAIOs must have the necessary skills, knowledge, training, and expertise to perform the responsibilities described in this section. At CFO Act agencies, a primary role of the CAIO must be coordination, innovation, and risk management for their agency’s use of AI specifically, as opposed to data or IT issues in general. Agencies may choose to designate an existing official, such as a Chief Information Officer (CIO), Chief Data Officer (CDO), Chief Technology Officer, or similar official with relevant or

¹¹ Given the importance of context-specific guidance on AI, agencies are encouraged to continue implementing their agency’s AI principles and guidelines, so long as they do not conflict with this memorandum.

complementary authorities and responsibilities, provided they have significant expertise in AI and meet the other requirements in this section.

- ii. **Responsibilities.** Executive Order 14110 tasks CAIOs with primary responsibility in their agencies, in coordination with other responsible officials, for coordinating their agency's use of AI, promoting AI innovation, managing risks from the use of AI, and carrying out the agency responsibilities defined in Section 8(c) of Executive Order 13960¹² and Section 4(b) of Executive Order 14091.¹³ In addition, CAIOs, in coordination with other responsible officials and appropriate stakeholders, are responsible for:

Coordinating Agency Use of AI

- A. serving as the senior advisor for AI to the head of the agency and other senior agency leadership and within their agency's senior decision-making forums;
- B. instituting the requisite governance and oversight processes to achieve compliance with this memorandum and enable responsible use of AI in the agency, in coordination with relevant agency officials;
- C. maintaining awareness of agency AI activities, including through the creation and maintenance of the annual AI use case inventory;
- D. developing a plan for compliance with this memorandum, as detailed in Section 3(a)(iii) of this memorandum, and an agency AI strategy, as detailed in Section 4(a) of this memorandum;
- E. working with and advising the agency CFO on the resourcing requirements necessary to implement this memorandum and providing recommendations on priority investment areas to build upon existing enterprise capacity;
- F. advising the Chief Human Capital Officer (CHCO) and where applicable, the Chief Learning Officer, on improving workforce capacity and securing and maintaining the skillsets necessary for using AI to further the agency's mission and adequately manage its risks;
- G. sharing relevant information with agency officials involved in the agency's major AI policymaking initiatives;
- H. supporting agency involvement with appropriate interagency coordination bodies related to their agency's AI activities, including representing the agency on the council described in Section 10.1(a) of Executive Order 14110;
- I. supporting and coordinating their agency's involvement in AI standards-setting bodies, as appropriate, and encouraging agency adoption of voluntary consensus standards for AI, as appropriate and consistent with OMB Circular No. A-119, if applicable;¹⁴

¹² Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, <https://www.govinfo.gov/content/pkg/FR-2020-12-08/pdf/2020-27065.pdf>.

¹³ Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, <https://www.govinfo.gov/content/pkg/FR-2023-02-22/pdf/2023-03779.pdf>.

¹⁴ OMB Circular A-119, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities* (Feb. 10, 1998), <https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf>.

- J. promoting equity and inclusion within the agency's AI governance structures and incorporating diverse perspectives into the decision-making process;

Promoting AI Innovation

- K. working with their agency to identify and prioritize appropriate uses of AI that will advance both their agency's mission and equitable outcomes;
- L. identifying and removing barriers to the responsible use of AI in the agency, including through the advancement of AI-enabling enterprise infrastructure, data access and governance, workforce development measures, policy, and other resources for AI innovation;
- M. working with their agency's CIO, CDO, and other relevant officials to ensure that custom-developed AI code and the data used to develop and test AI are appropriately inventoried, shared, and released in agency code and data repositories in accordance with Section 4(d) of this memorandum;
- N. advocating within their agency and to the public on the opportunities and benefits of AI to the agency's mission;

Managing Risks from the Use of AI

- O. managing an agency program that supports the enterprise in identifying and managing risks from the use of AI, especially for safety-impacting and rights-impacting AI;
- P. working with relevant senior agency officials to establish or update processes to measure, monitor, and evaluate the ongoing performance and effectiveness of the agency's AI applications and whether the AI is advancing the agency's mission and meeting performance objectives;
- Q. overseeing agency compliance with requirements to manage risks from the use of AI, including those established in this memorandum and in relevant law and policy;
- R. conducting risk assessments, as necessary, of the agency's AI applications to ensure compliance with this memorandum;
- S. working with relevant agency officials to develop supplementary AI risk management guidance particular to the agency's mission, including working in coordination with officials responsible for privacy and civil rights and civil liberties on identifying safety-impacting and rights-impacting AI within the agency;
- T. waiving individual applications of AI from elements of Section 5 of this memorandum through the processes detailed in that section; and
- U. in partnership with relevant agency officials (e.g., authorizing, procurement, legal, data governance, human capital, and oversight officials), establishing controls to ensure that their agency does not use AI that is not in compliance with this memorandum, including by assisting these relevant agency officials in evaluating Authorizations to Operate based on risks from the use of AI.

- iii. **Seniority.** For CFO Act agencies, the CAIO must be a position at the Senior Executive Service, Scientific and Professional, or Senior Leader level, or equivalent. In other agencies, the CAIO must be at least a GS-15 or equivalent.
- iv. **Position and Reporting Structure.** CAIOs must have the necessary authority to perform the responsibilities in this section and must be positioned highly enough to engage regularly with other agency leadership, to include the Deputy Secretary or equivalent. Further, CAIOs must coordinate with other responsible officials at their agency to ensure that the agency's use of AI complies with and is appropriate in light of applicable law and governmentwide guidance.

c. Internal Agency AI Coordination

Agencies must ensure that AI issues receive adequate attention from the agency's senior leadership. Consistent with Section 10.1(b) of Executive Order 14110, agencies must take appropriate steps, such as through the convening of an AI governance body, to coordinate internally among officials responsible for aspects of AI adoption and risk management. Likewise, the CAIO must be involved, at appropriate times, in broader agency-wide risk management bodies and processes,¹⁵ including in the development of the agency risk management strategy.¹⁶ The agency's AI coordination mechanisms should be aligned to the needs of the agency based on, for example, the degree to which the agency currently uses AI, the degree to which AI could improve the agency's mission, and the risks posed by the agency's current and potential uses of AI.

Each CFO Act agency is required to establish an AI Governance Board to convene relevant senior officials to govern the agency's use of AI, including to remove barriers to the use of AI and to manage its associated risks. Those agencies are permitted to rely on existing governance bodies¹⁷ to fulfill this requirement as long as they currently satisfy or are made to satisfy both of the following:

- i. Agency AI Governance Boards must be chaired by the Deputy Secretary of the agency or equivalent and vice-chaired by the agency CAIO, and these roles should not be assigned to other officials. The full Board, including the Deputy Secretary, must convene on at least a semi-annual basis. Working through this Board, CAIOs will support their respective Deputy Secretaries in coordinating AI activities across the agency and implementing relevant sections of Executive Order 14110.

¹⁵ See, e.g., OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf.

¹⁶ See OMB Circular No. A-130, *Managing Information as a Strategic Resource*, Appx. I, sec. 5(b) (July 28, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

¹⁷ An example of a qualifying body includes agency Data Governance Bodies, established by OMB Memorandum M-19-23, *Phase I Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, <https://www.whitehouse.gov/wp-content/uploads/2019/07/m-19-23.pdf>.

- ii. Agency AI Governance Boards must include appropriate representation from senior agency officials responsible for key enablers of AI adoption and risk management, including at least IT, cybersecurity, data, privacy, civil rights and civil liberties, equity, statistics, human capital, procurement, budget, legal, agency management, customer experience, program evaluation, and officials responsible for implementing AI within an agency's program office(s). Agencies should also consider including representation from their respective Office of the Inspector General.

Agencies are encouraged to have their AI Governance Boards consult external experts as appropriate and consistent with applicable law. Experts' individual viewpoints can help broaden the perspective of an existing governance board and inject additional technical, ethics, civil rights and civil liberties, or sector-specific expertise, as well as methods for engaging the workforce.

4. ADVANCING RESPONSIBLE ARTIFICIAL INTELLIGENCE INNOVATION

If implemented responsibly, AI can improve operations and deliver efficiencies across the Federal Government. Agencies must improve their ability to use AI in ways that benefit the public and increase mission effectiveness, while recognizing the limitations and risks of AI and when it is not suited for a given task. In particular, agencies are encouraged to prioritize AI development and adoption for the public good and where the technology can be helpful in understanding and tackling large societal challenges, such as using AI to improve the accessibility of government services, reduce food insecurity, address the climate crisis, improve public health, advance equitable outcomes, protect democracy and human rights, and grow economic competitiveness in a way that benefits people across the United States.

To achieve this, agencies should build upon existing internal enterprise capacity to support responsible AI innovation, take actions to strengthen their AI and AI-enabling talent,¹⁸ and improve their ability to develop and procure AI. Agencies should both explore joint efforts to scale these opportunities as well as take steps to responsibly share their AI resources across the Federal Government and with the public.

a. AI Strategies

Within 365 days of the issuance of this memorandum, each CFO Act agency must develop and release publicly on the agency's website a strategy for identifying and removing barriers to the responsible use of AI and achieving enterprise-wide improvements in AI maturity, including:

- i. the agency's current and planned uses of AI that are most impactful to an agency's mission or service delivery;¹⁹

¹⁸ Agencies should also ensure that they consider and satisfy applicable collective bargaining obligations regarding their implementation of AI.

¹⁹ Consistent with Sections 7225(d) and 7228 of the Advancing American AI Act, this requirement applies to CFO Act agencies except for the Department of Defense, and does not apply to elements of the Intelligence Community,

- ii. a current assessment of the agency's AI maturity and the agency's AI maturity goals;
- iii. the agency's plans to effectively govern its use of AI, including through its Chief AI Officer, AI Governance Boards, and improvements to its AI use case inventory;
- iv. a plan for developing sufficient enterprise capacity for AI innovation, including mature AI-enabling infrastructure for the data, computing, development, testing, cybersecurity compliance, deployment, and continuous-monitoring infrastructure necessary to build, test, and maintain AI;
- v. a plan for providing sufficient AI tools and capacity to support the agency's research and development (R&D) work consistent with the R&D priorities developed by OMB and the Office of Science and Technology Policy, the National AI R&D Strategic Plan, and agency-specific R&D plans;
- vi. a plan for establishing operational and governance processes as well as developing the necessary infrastructure to manage risks from the use of AI;
- vii. a current assessment of the agency's AI and AI-enabling workforce capacity and projected AI and AI-enabling workforce needs, as well as a plan to recruit, hire, train, retain, and empower AI practitioners and achieve AI literacy for non-practitioners involved in AI to meet those needs;
- viii. the agency's plan to encourage diverse perspectives throughout the AI development or procurement lifecycle, including how to determine whether a particular use of AI is meeting the agency's equity goals and civil rights commitments; and
- ix. specific, prioritized areas and planning for future AI investment, leveraging the annual budget process as appropriate.

b. Removing Barriers to the Responsible Use of AI

Embracing innovation requires removing unnecessary and unhelpful barriers to the use of AI while retaining and strengthening the guardrails that ensure its responsible use. Agencies should create internal environments where those developing and deploying AI have sufficient flexibility and where limited AI resources and expertise are not diverted away from AI innovation and risk management. Agencies should take steps to remove barriers to responsible use of AI, paying special attention to the following recommendations:

- i. **IT Infrastructure.** Agencies should ensure that their AI projects have access to adequate IT infrastructure, including high-performance computing infrastructure specialized for AI training and inference, where necessary. Agencies should also ensure adequate access for AI developers to the software tools, open-source libraries, and deployment and

as defined in 50 U.S.C. § 3003(4). Information that would be protected from release if requested under 5 U.S.C. § 552 need not be included in the strategy.

monitoring capabilities necessary to rapidly develop, test, and maintain AI applications.

- ii. **Data.** Agencies should develop adequate infrastructure and capacity to sufficiently share, curate, and govern agency data for use in training, testing, and operating AI. This includes an agency's capacity to maximize appropriate access to and sharing of both internally held data and agency data managed by third parties. Agencies should also explore the possible utility of and legal authorities supporting the use of publicly available information, and encourage its use where appropriate and consistent with the data practices outlined in this memorandum. Any data used to help develop, test, or maintain AI applications, regardless of source, should be assessed for quality, representativeness, and bias. These activities should be supported by resources to enable sound data governance and management practices, particularly as they relate to data collection, curation, labeling, and stewardship.
- iii. **Cybersecurity.** Agencies should update, as necessary, processes for information system authorization and continuous monitoring to better address the needs of AI applications, including to advance the use of continuous authorizations for AI. Consistent with Section 10.1(f) of Executive Order 14110, agency authorizing officials are encouraged to prioritize review of generative AI and other critical and emerging technologies in Authorizations to Operate and any other applicable release or oversight processes.
- iv. **Generative AI.** In addition to following the guidance provided in Section 10.1(f) of Executive Order 14110, agencies should assess potential beneficial uses of generative AI in their missions and establish adequate safeguards and oversight mechanisms that allow generative AI to be used in the agency without posing undue risk.

c. AI Talent

Consistent with Section 10.2 of Executive Order 14110, agencies are strongly encouraged to prioritize recruiting, hiring, developing, and retaining talent in AI and AI-enabling roles to increase enterprise capacity for responsible AI innovation. Agencies should:

- i. follow the hiring practices described in the forthcoming AI and Tech Hiring Playbook created by the Office of Personnel Management (OPM), including encouraging applications from individuals with diverse perspectives, making best use of available hiring and retention authorities and using descriptive job titles and skills-based assessments;
- ii. designate an AI Talent Lead who, for at least the duration of the AI Talent Task Force, will be accountable for reporting to agency leadership, tracking AI hiring across the agency, and providing data to OPM and OMB on hiring needs and progress. The AI Talent Task Force, established in Section 10.2(b) of EO 14110, will provide AI Talent Leads with engagement opportunities to enhance their AI hiring practices and to drive impact through collaboration across agencies, including sharing position descriptions, coordinating marketing and outreach, shared hiring actions, and, if appropriate, sharing

applicant information across agencies; and

- iii. in consultation with Federal employees and their union representatives, where applicable, provide resources and training to develop AI talent internally and increase AI training offerings for Federal employees, including opportunities that provide Federal employees pathways to AI occupations and that assist employees affected by the application of AI to their work.

d. AI Sharing and Collaboration

Openness, sharing, and reuse of AI significantly enhance both innovation and transparency, and must also be done responsibly to avoid undermining the rights, safety, and security of the public. Agencies must share their AI code, models, and data, and do so in a manner that facilitates re-use and collaboration Government-wide and with the public, subject to applicable law, governmentwide guidance, and the following considerations:

- i. **Sharing and Releasing AI Code and Models.** Agencies must proactively share their custom-developed code²⁰—including models and model weights—for AI applications in active use and must release and maintain that code as open source software on a public repository,²¹ unless:
 - A. the sharing of the code is restricted by law or regulation, including patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulations, and Federal laws and regulations governing classified information;
 - B. the sharing of the code would create an identifiable risk to national security, confidentiality of Government information, individual privacy, or the rights or safety of the public;
 - C. the agency is prevented by a contractual obligation from doing so; or
 - D. the sharing of the code would create an identifiable risk to agency mission, programs, or operations, or to the stability, security, or integrity of an agency’s systems or personnel.

Agencies should prioritize sharing custom-developed code, such as commonly used packages or functions, that has the greatest potential for re-use by other agencies or the public.

- ii. **Sharing and Releasing AI Data Assets.** Data used to develop and test AI is likely to constitute a “data asset” for the purposes of implementing the Open, Public, Electronic

²⁰ A full definition for “custom-developed code” is provided in Section 6.

²¹ For guidance and best practices related to sharing code and releasing it as open source, agencies should consult OMB Memorandum M-16-21, *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (Aug. 8, 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_21.pdf. Agencies are additionally encouraged to draw upon existing collaboration methods to facilitate the sharing and release of code and models, including the council described in Section 10.1(a) of Executive Order 14110, the General Services Administration’s AI Community of Practice, and <https://www.code.gov>, as well as other publicly available code repositories.

and Necessary (OPEN) Government Data Act,²² and agencies must, if required by that Act and pursuant to safety and security considerations in Section 4.7 of Executive Order 14110, release such data assets publicly as open government data assets.²³ When sharing AI data assets, agencies should promote data interoperability, including by coordinating internally and with other relevant agencies on interoperability criteria and using standardized data formats where feasible and appropriate.

- iii. **Partial Sharing and Release.** Where some portion of an AI project's code, models, or data cannot be shared or released publicly pursuant to subsections (i) and (ii) of this section, the rest should still be shared or released where practicable, such as by releasing the data used to evaluate a model even if the model itself cannot be safely released, or by sharing a model within the Federal Government even if the model cannot be publicly released. Where code, models, or data cannot be released without restrictions on who can access it, agencies should also, where practicable, share them through Federally controlled infrastructure that allows controlled access by entities outside the Federal Government, such as via the National AI Research Resource.
- iv. **Procuring AI for Sharing and Release.** When procuring custom-developed code for AI, data to train and test AI, and enrichments to existing data (such as labeling services), agencies are encouraged to do so in a manner that allows for the sharing and public release of the relevant code, models, and data.
- v. **Unintended Disclosure of Data from AI Models.** When agencies are deciding whether to share and release AI models and model weights, they should assess the risk that the models can be induced to reveal sensitive details of the data used to develop them. Agencies' assessment of risk should include a model-specific risk analysis.²⁴

e. Harmonization of Artificial Intelligence Requirements

Interpreting and implementing AI management requirements in a consistent manner across Federal agencies will create efficiencies as well as opportunities for sharing resources and best practices. To assist in this effort and consistent with Section 10.1(a) of Executive Order 14110, OMB, in collaboration with the Office of Science and Technology Policy, will coordinate the development and use of AI in agencies' programs and operations—including the implementation of this memorandum—across Federal agencies through an interagency council. This will include at a minimum:

- i. promoting shared templates and formats;
- ii. sharing best practices and lessons learned, including for achieving meaningful participation from affected communities and the public in AI development and

²² Title II of the Foundations for Evidence-Based Policymaking Act of 2018, P.L. 115-435.

²³ Where such data is already publicly available, agencies are not required to duplicate it, but should maintain and share the provenance of such data and how others can access it.

²⁴ The risks of unintended disclosure differ by model, and agencies should also not assume that an AI model poses the same privacy and confidentiality risks as the data used to develop it.

procurement, updating organizational processes to better accommodate AI, removing barriers to responsible AI innovation, responding to AI incidents that may have resulted in harm to an individual, and building a diverse AI workforce to meet the agency's needs;

- iii. sharing technical resources for implementation of this memorandum's risk management practices, such as for testing, continuous monitoring, and evaluation; and
- iv. highlighting exemplary uses of AI for agency adoption, particularly uses which help address large societal challenges.

5. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

Agencies have a range of policies, procedures, and officials in place to manage risks related to agency information and systems. To better address risks from the use of AI, and particularly risks to the rights and safety of the public, all agencies are required to implement minimum practices, detailed below, to manage risks from safety-impacting AI and rights-impacting AI.²⁵ However, Section 5(a) through (c) of this memorandum do not apply to elements of the Intelligence Community.²⁶

a. Actions

- i. **Implementation of Risk Management Practices and Termination of Non-Compliant AI.** By December 1, 2024, agencies must implement the minimum practices in Section 5(c) of this memorandum for safety-impacting and rights-impacting AI, or else stop using any AI in their operations that is not compliant with the minimum practices, consistent with the details and caveats in that section.
- ii. **Certification and Publication of Determinations and Waivers.** By December 1, 2024, and annually thereafter, each agency must certify the ongoing validity of the determinations made under subsection (b) and the waivers granted under subsection (c) of this section. To the extent consistent with law and governmentwide policy, the agency must publicly release a summary detailing each individual determination and waiver, as well its justification. Alternatively, if an agency has no active determinations or waivers, it must publicly indicate that fact and report it to OMB. OMB will issue detailed instructions for these summaries through its Integrated Data Collection process or an OMB-designated successor process.

²⁵ Agencies are not required to incorporate these practices into criteria for granting federal financial assistance (FFA). However, they are encouraged, consistent with applicable law, to consider the minimum practices when choosing such criteria.

²⁶ Although elements of the Intelligence Community are not required to implement these practices, they are encouraged to do so.

b. Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting

All AI that matches the definitions of “safety-impacting AI” or “rights-impacting AI” as defined in Section 6 must follow the minimum practices in Section 5(c) by the applicable deadline. Agencies must review each current or planned use of AI to assess whether it matches the definition of safety-impacting AI or rights-impacting AI. When conducting such an assessment, as reflected by the definitions of safety-impacting AI and rights-impacting AI in Section 6 of this memorandum, agencies must look to whether the particular AI output serves as a principal basis for a decision or action.

Additionally, AI used for one of the purposes identified in Appendix I is automatically *presumed* to be safety-impacting or rights-impacting. However, the agency CAIO, in coordination with other relevant officials, may determine (or revisit a prior determination) that a particular AI application or component²⁷ subject to this presumption does not match the definitions of “safety-impacting AI” or “rights-impacting AI” and is therefore not subject to the minimum practices. The agency CAIO may make or revisit such a determination only with a documented context-specific and system-specific risk assessment and may revisit a prior determination at any time. This responsibility shall not be delegated to other officials. In addition to the certification and publication requirements in Section 5(a)(ii) of this memorandum, CAIOs must centrally track these determinations, reassess them if there are significant changes to the conditions or context in which the AI is used, and report to OMB within 30 days of making or changing a determination, detailing the scope, justification, and supporting evidence.

c. Minimum Practices for Safety-Impacting and Rights-Impacting Artificial Intelligence

Except as prevented by applicable law and governmentwide guidance, agencies must apply the minimum risk management practices in this section to safety-impacting and rights-impacting AI by December 1, 2024, or else stop using the AI until they achieve compliance. Prior to December 1, 2024, agency CAIOs should work with their agencies’ relevant officials to bring potentially non-compliant AI into conformity, which may include requests that third-party vendors voluntarily take appropriate action (e.g., via updated documentation or testing measures). To ensure compliance with this requirement, relevant agency officials must use existing mechanisms wherever possible, (for example, the Authorization to Operate process).²⁸ An agency may also request an extension or grant a waiver to this requirement through its CAIO using the processes detailed below.

²⁷ CAIOs may also make these determinations across groups of AI applications or components that are closely related by design or deployment context, provided that: (1) those systems have undergone a risk assessment that adequately considers the risks from each individual system or from all possible systems in the group; and (2) the systems are substantially identical in their risk profiles.

²⁸ While agencies must use existing authorization and oversight processes to enforce these practices, the practices are most effective when applied early in the research, design, and development of AI systems, and agencies should plan for and adopt the practices throughout the relevant AI systems’ lifecycles and as early as possible, as appropriate.

Agencies must document their implementation of these practices and be prepared to report them to OMB, either as a component of the annual AI use case inventory, periodic accountability reviews, or upon request as determined by OMB.

The practices in this section represent an initial baseline for managing risk from the use of AI. Agencies must identify additional context-specific risks that are associated with their use of AI and address them as appropriate. Such risk considerations may include impacts to safety, security, civil rights, civil liberties, privacy, democratic values, human rights, equal opportunities, worker well-being, access to critical resources and services, agency trust and credibility, and market competition. To address these potential risk management gaps, agencies are encouraged to promote and to incorporate, as appropriate, additional best practices for AI risk management, such as from the National Institute of Standards and Technology (NIST) AI Risk Management Framework,²⁹ the Blueprint for an AI Bill of Rights,³⁰ relevant international standards,³¹ and the workforce principles and best practices for employers established pursuant to Section 6(b)(i) of Executive Order 14110. Agencies are also encouraged to continue developing their own agency-specific practices, as appropriate and consistent with this memorandum and the principles in Executive Order 13960, Executive Order 14091, and Executive Order 14110.

The practices in this section also do not supersede, modify, or direct an interpretation of existing requirements mandated by law or governmentwide policy, and responsible agency officials must coordinate to ensure that the adoption of these practices does not conflict with other applicable law or governmentwide guidance.

- i. **Exclusions from Minimum Practices.** Agencies are not required to follow the minimum practices outlined in this section when using AI *solely* to:
 - A. evaluate a potential vendor, commercial capability, or freely available AI capability that is not otherwise used in agency operations, exclusively for the purpose of making a procurement or acquisition decision; or
 - B. achieve its conformity with the requirements of this section, such as using an AI application in controlled testing conditions to carry out the minimum testing requirements below.³²
- ii. **Extensions for Minimum Practices.** Agencies may request from OMB an extension of up to one year, for a particular use of AI that cannot feasibly meet the minimum requirements in this section by that date. OMB will not grant renewals beyond the initial one-year extension. Any extension requests shall be submitted prior to October 15, 2024. The request must be accompanied by a detailed justification for why the agency cannot achieve compliance for the use of AI in question and what practices the agency has in

²⁹ *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST Publication AI 100-1, <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

³⁰ *Blueprint for an AI Bill of Rights*, White House Office of Science and Technology Policy, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

³¹ For example, ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management, <https://www.iso.org/standard/77304.html>.

³² This exclusion must not be applied to any use of AI in real-world conditions, except as specifically allowed by this section.

place to mitigate the risks from noncompliance, as well as a plan for how the agency will come to implement the full set of required minimum practices from this section. OMB will issue detailed instructions for extension requests through its Integrated Data Collection process or an OMB-designated successor process.

- iii. **Waivers from Minimum Practices.** In coordination with other relevant officials, an agency CAIO may waive one or more of the requirements in this section for a specific covered AI application or component³³ after making a written determination, based upon a system-specific and context-specific risk assessment, that fulfilling the requirement would increase risks to safety or rights overall or would create an unacceptable impediment to critical agency operations. An agency CAIO may also revoke a previously issued waiver at any time. This responsibility shall not be delegated to other officials. In addition to the certification and publication requirements in Section 5(a)(ii) of this memorandum, CAIOs must centrally track waivers, reassess them if there are significant changes to the conditions or context in which the AI is used, and report to OMB within 30 days of granting or revoking any waiver, detailing the scope, justification, and supporting evidence.
- iv. **Minimum Practices for Either Safety-Impacting or Rights-Impacting AI.** No later than December 1, 2024, agencies must follow these practices *before* using new or existing covered safety-impacting or rights-impacting AI:
 - A. **Complete an AI impact assessment.** Agencies should update their impact assessments periodically and leverage them throughout the AI's lifecycle. In their impact assessments, agencies must document at least the following:
 - 1. *The intended purpose for the AI and its expected benefit*, supported by specific metrics or qualitative analysis. Metrics should be quantifiable measures of positive outcomes for the agency's mission—for example to reduce costs, wait time for customers, or risk to human life—that can be measured using performance measurement or program evaluation methods after the AI is deployed to demonstrate the value of using AI.³⁴ Where quantification is not feasible, qualitative analysis should demonstrate an expected positive outcome, such as for improvements to customer experience, and it should demonstrate that AI is better suited to accomplish the relevant task as compared to alternative strategies.
 - 2. *The potential risks of using AI*, as well as what, if any, additional mitigation measures, beyond these minimum practices, the agency will take to help

³³ CAIOs may also grant waivers applicable to groups of AI applications or components that are closely related by design or deployment context, provided that: (1) those systems have undergone a risk assessment that adequately considers the risks from each individual system or from all possible systems in the group; and (2) the systems are substantially identical in their risk profiles.

³⁴ For supervised and semi-supervised AI, agencies should use a target variable which can be reliably measured and adequately represents the desired real-world outcomes.

reduce these risks. Agencies should document the stakeholders³⁵ who will be most impacted by the use of the system and assess the possible failure modes of the AI and of the broader system, both in isolation and as a result of human users and other likely variables outside the scope of the system itself. Agencies should be especially attentive to the potential risks to underserved communities. The expected benefits of the AI functionality should be considered against its potential risks, and if the benefits do not meaningfully outweigh the risks, agencies should not use the AI.

3. *The quality and appropriateness of the relevant data.* Agencies must assess the quality of the data used in the AI's design, development, training, testing, and operation and its fitness to the AI's intended purpose. In conducting assessments, if the agency cannot obtain such data after a reasonable effort to do so, it must obtain sufficient descriptive information from the vendor (e.g., AI or data provider) to satisfy the reporting requirements in this paragraph. At a minimum, agencies must document:
 - a. the data collection and preparation process, which must also include the provenance of any data used to train, fine-tune, or operate the AI;
 - b. the quality³⁶ and representativeness³⁷ of the data for its intended purpose;
 - c. how the data is relevant to the task being automated and may reasonably be expected to be useful for the AI's development, testing, and operation;
 - d. whether the data contains sufficient breadth to address the range of real-world inputs the AI might encounter and how data gaps and shortcomings have been addressed either by the agency or vendor; and
 - e. if the data is maintained by the Federal Government, whether that data is publicly disclosable as an open government data asset, in accordance with applicable law and policy.³⁸

- B. **Test the AI for performance in a real-world context.** Agencies must conduct adequate testing to ensure the AI, as well as components that rely on it, will work in its intended real-world context. Such testing should follow domain-specific best practices, when available, and should take into account both the specific technology used and feedback from human operators, reviewers, employees, and

³⁵ Stakeholders will vary depending on how AI is being used. For example, if an agency is using AI to control a water treatment process, stakeholders may include (1) local residents; (2) state, local, tribal, and territorial government representatives; and (3) environmental experts.

³⁶ Consistent with OMB Memorandum M-19-15, *Improving Implementation of the Information Quality Act*, <https://www.whitehouse.gov/wp-content/uploads/2019/04/M-19-15.pdf>, if applicable. Agencies should also consider the National Science and Technology Council's report *Protecting the Integrity of Government Science*, https://www.whitehouse.gov/wp-content/uploads/2022/01/01-22-Protecting_the_Integrity_of_Government_Science.pdf.

³⁷ Agencies should assess whether the data used can produce or amplify inequitable outcomes as a result of poor data representativeness or harmful bias. Such outcomes can result from historical discrimination, such as the perpetuation of harmful gender-based and racial stereotypes in society.

³⁸ See 44 U.S.C. § 3502(20).

customers who use the service or are impacted by the system's outcomes. Testing conditions should mirror as closely as possible the conditions in which the AI will be deployed. Through test results, agencies should demonstrate that the AI will achieve its expected benefits and that associated risks will be sufficiently mitigated, or else the agency should not use the AI. In conducting such testing, if an agency does not have access to the underlying source code, models, or data, the agency must use alternative test methodologies, such as querying the AI service and observing the outputs or providing evaluation data to the vendor and obtaining results. Agencies are also encouraged to leverage pilots and limited releases, with strong monitoring, evaluation, and safeguards in place, to carry out the final stages of testing before a wider release.

- C. **Independently evaluate the AI.** Agencies, through the CAIO, an agency AI oversight board, or other appropriate agency office with existing test and evaluation responsibilities, must review relevant AI documentation to ensure that the system works appropriately and as intended, and that its expected benefits outweigh its potential risks. At a minimum, this documentation must include the completed impact assessment and results from testing AI performance in a real-world context referenced in paragraphs (A) and (B) of this subsection. Agencies must incorporate this independent evaluation into an applicable release or oversight process, such as the Authorization to Operate process. The independent reviewing authority must not have been directly involved in the system's development.

No later than December 1, 2024 and on an ongoing basis *while* using new or existing covered safety-impacting or rights-impacting AI, agencies must ensure these practices are followed for the AI:

- D. **Conduct ongoing monitoring.** In addition to pre-deployment testing, agencies must institute ongoing procedures to monitor degradation of the AI's functionality and to detect changes in the AI's impact on rights and safety. Agencies should also scale up the use of new or updated AI features incrementally where possible to provide adequate time to monitor for adverse performance or outcomes. Agencies should monitor and defend the AI from AI-specific exploits,³⁹ particularly those that would adversely impact rights and safety.
- E. **Regularly evaluate risks from the use of AI.** The monitoring process in paragraph (D) must include periodic human reviews to determine whether the deployment context, risks, benefits, and agency needs have evolved. Agencies must also determine whether the current implementation of the memorandum's minimum practices adequately mitigates new and existing risks, or whether

³⁹ For example, the AI-specific exploits outlined in the MITRE ATLAS framework, see <https://atlas.mitre.org/> and NIST's taxonomy for adversarial machine learning, see <https://csrc.nist.gov/pubs/ai/100/2/e2023/final>.

updated risk response options are required.⁴⁰ At a minimum, human review is required at least on an annual basis and after significant modifications to the AI or to the conditions or context in which the AI is used, and the review must include renewed testing for performance of the AI in a real-world context.⁴¹ Reviews must also include oversight and consideration by an appropriate internal agency authority not directly involved in the system's development or operation.

- F. **Mitigate emerging risks to rights and safety.** Upon identifying new or significantly altered risks to rights or safety through ongoing monitoring, periodic review, or other mechanisms, agencies must take steps to mitigate those risks, including, as appropriate, through updating the AI to reduce its risks or implementing procedural or manual mitigations, such as more stringent human intervention requirements. As significant modifications make the existing implementation of the other minimum practices in this section less effective, such as by making training or documentation inaccurate, agencies must update or repeat those practices, as appropriate. Where the AI's risks to rights or safety exceed an acceptable level and where mitigation strategies do not sufficiently reduce risk, agencies must stop using the AI as soon as is practicable.⁴²
- G. **Ensure adequate human training and assessment.** Agencies must ensure there is sufficient training, assessment, and oversight for operators of the AI to interpret and act on the AI's output, combat any human-machine teaming issues (such as automation bias), and ensure the human-based components of the system effectively manage risks from the use of AI. Training should be conducted on a periodic basis, determined by the agency, and should be specific to the AI product or service being operated and how it is being used.
- H. **Provide additional human oversight, intervention, and accountability as part of decisions or actions that could result in a significant impact on rights or safety.** Agencies must assess their rights-impacting and safety-impacting uses of AI to identify any decisions or actions in which the AI is not permitted to act without additional human oversight, intervention, and accountability. When immediate human intervention is not practicable for such an action or decision, agencies must ensure that the AI functionality has an appropriate fail-safe that minimizes the risk of significant harm.⁴³

⁴⁰ In some cases, this may require a program evaluation, as defined under requirements of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435, to determine the extent to which the AI is advancing the agency's mission and objectives.

⁴¹ For customer-facing services, agencies should consider customer feedback in their human review criteria.

⁴² Agencies are responsible for determining how to safely decommission AI that was already in use at the time of this memorandum's release, without significant disruptions to essential government functions.

⁴³ For example, an AI-enabled safety mechanism may require an immediate and automated action to prevent a harm from occurring. It would not be practicable in this case to require human intervention to approve the activation of the safety mechanism. However, agencies must still determine the appropriate oversight and accountability processes for such a use of AI.

- I. **Provide public notice and plain-language documentation.** Agencies must ensure, to the extent consistent with applicable law and governmentwide guidance, including concerning protection of privacy and of sensitive law enforcement, national security, and other protected information, that the AI's entry in the use case inventory provides accessible documentation in plain language of the system's functionality to serve as public notice of the AI to its users and the general public. Where people interact with a service relying on the AI and are likely to be impacted by the AI, agencies must also provide reasonable and timely notice⁴⁴ about the use of the AI and a means to directly access any public documentation about it in the use case inventory. Where agencies' use cases are not included in their public inventories, they may still be required to report relevant information to OMB and must ensure adequate transparency in their use of AI, as appropriate and consistent with applicable law.
- v. **Additional Minimum Practices for Rights-Impacting AI.**

No later than December 1, 2024, agencies must follow the above minimum practices for AI that is *either* safety-impacting *or* rights-impacting. In addition, no later than December 1, 2024, agencies must also follow these minimum practices *before* initiating use of new or existing rights-impacting AI:

 - A. **Identify and assess AI's impact on equity and fairness, and mitigate algorithmic discrimination when it is present.** Agencies must:
 1. Identify and document in their AI impact assessment when using data that contains information about a class protected by Federal nondiscrimination laws (e.g., race, age, etc.). Given the risks arising when AI may correlate demographic information with other types of information, agencies should also assess and document whether the AI model could foreseeably use other attributes as proxies for a protected characteristic and whether such use would significantly influence model performance;
 2. Assess the AI in a real-world context to determine whether the AI model results in significant disparities in the model's performance (e.g., accuracy, precision, reliability in predicting outcomes) across demographic groups;
 3. Mitigate disparities that lead to, or perpetuate, unlawful discrimination or harmful bias, or that decrease equity as a result of the government's use of the AI; and
 4. Consistent with applicable law, cease use of the AI for agency decision-making if the agency is unable to adequately mitigate any associated risk of unlawful discrimination against protected classes. Agencies should maintain appropriate documentation to accompany this decision-making, and should disclose it publicly to the extent consistent with applicable law and governmentwide policy.

⁴⁴ Wherever feasible, agencies should provide notice to a user before the AI takes an action that significantly impacts them.

B. Consult and incorporate feedback from affected communities and the public.

Consistent with applicable law and governmentwide guidance, agencies must consult affected communities, including underserved communities, and they must solicit public feedback, where appropriate, in the design, development, and use of the AI and use such feedback to inform agency decision-making regarding the AI. The consultation and feedback process must include seeking input on the agency's approach to implementing the minimum risk management practices established in Section 5(c) of this memorandum, such as applicable opt-out procedures. Agencies should consider and manage the risks of public consultation in contexts like fraud prevention and law enforcement investigations, where consulting with the targeted individual is impractical but consulting with a representative group may be appropriate.⁴⁵

Agencies are strongly encouraged to solicit feedback on an ongoing basis from affected communities in particular as well as from the public broadly, especially after significant modifications to the AI or the conditions or context in which it is used.⁴⁶ In the course of assessing such feedback, if an agency determines that the use of AI in a given context would cause more harm than good, the agency should not use the AI.

To carry out such consultations and feedback processes, agencies must take appropriate steps to solicit input from the communities and individuals affected by the AI, which could include:⁴⁷

1. direct usability testing, such as observing users interacting with the system;
2. general solicitations of comments from the public, such as a request for information in the *Federal Register* or a "Tell Us About Your Experience" sheet with an open-ended space for responses;
3. post-transaction customer feedback collections;⁴⁸
4. public hearings or meetings, such as a listening session;
5. outreach to relevant Federal employee groups and Federal labor organizations, including on the appropriate fulfillment of collective bargaining obligations, where applicable; or
6. any other transparent process that seeks public input, comments, or feedback from the affected groups in a meaningful, equitable, accessible,

⁴⁵ For example, an agency using an AI tool to detect Federal benefits fraud is not required to consult with the target of their investigation. However, an agency should discern when it is appropriate to consult with civil society groups, academia, or other experts in the field to understand the technology's impact.

⁴⁶ The affected communities will vary depending on an agency's deployment context, but may include customers (for example, individuals, businesses, or organizations that interact with an agency) or Federal employee groups and employees' union representatives, when applicable.

⁴⁷ Agencies are encouraged to engage with OMB on whether they are required to submit information collection requests for OMB clearance under the Paperwork Reduction Act (44 U.S.C. § 3507) for the purposes of these consultations and feedback processes.

⁴⁸ Information on post-transaction customer feedback surveys can be found in OMB Circular A-11, Section 280 – Managing Customer Experience and Improving Service Delivery, <https://www.whitehouse.gov/wp-content/uploads/2018/06/s280.pdf>.

and effective manner.

No later than December 1, 2024 and on an ongoing basis *while* using new or existing covered rights-impacting AI, agencies must ensure these practices are followed for the AI:

- C. **Conduct ongoing monitoring and mitigation for AI-enabled discrimination.** As part of the ongoing monitoring requirement established in Section 5(c)(iv)(D), agencies must also monitor rights-impacting AI to specifically assess and mitigate AI-enabled discrimination against protected classes, including discrimination that might arise from unforeseen circumstances, changes to the system after deployment, or changes to the context of use or associated data. Where sufficient mitigation is not possible, agencies must safely discontinue use of the AI functionality.
- D. **Notify negatively affected individuals.** Consistent with applicable law and governmentwide guidance, agencies must notify individuals when use of the AI results in an adverse decision or action that specifically concerns them, such as the denial of benefits or deeming a transaction fraudulent.⁴⁹ Agencies should consider the timing of their notice and when it is appropriate to provide notice in multiple languages and through alternative formats and channels, depending on the context of the AI's use. The notice must also include a clear and accessible means of contacting the agency and, where applicable, provide information to the individual on their right to appeal. Agencies must also abide by any existing obligations to provide explanations for such decisions and actions.⁵⁰
- E. **Maintain human consideration and remedy processes.** Where practicable and consistent with applicable law and governmentwide guidance, agencies must provide timely human consideration and potential remedy, if appropriate, to the use of the AI via a fallback and escalation system in the event that an impacted individual would like to appeal or contest the AI's negative impacts on them. Agencies that already maintain an appeal or secondary human review process for adverse actions, or for agency officials' substantive or procedural errors, can leverage and expand such processes, as appropriate, or establish new processes to meet this requirement. These remedy processes should not place unnecessary burden on the impacted individual, and agencies should follow OMB guidance on

⁴⁹ In some instances, such as an active law enforcement investigation, providing immediate notice may be inappropriate or impractical, or disclosure may be more appropriate at a later stage (for example, prior to a defendant's trial).

⁵⁰ Explanations might include, for example, how and why the AI-driven decision or action was taken. This does not mean that agencies must provide a perfect breakdown of how a machine learning system came to a conclusion, as exact explanations of AI decisions may not be technically feasible. However, agencies should still characterize the general nature of such AI decisions through context such as the data that the decision relied upon, the design of the AI, and the broader decision-making context in which the system operates. Such explanations should be technologically valid, meaningful, useful, and as simply stated as possible, and higher-risk decisions should be accompanied by more comprehensive explanations.

calculating administrative burden.⁵¹ Whenever agencies are unable to provide an opportunity for an individual to appeal due to law, governmentwide guidance, or impracticability, they must create appropriate alternative mechanisms for human oversight of the AI.

- F. **Maintain options to opt-out for AI-enabled decisions.** Agencies must provide and maintain a mechanism for individuals to conveniently opt-out from the AI functionality in favor of a human alternative, where practicable and consistent with applicable law and governmentwide guidance. An opt-out mechanism must be prominent, readily available, and accessible, and it is especially critical where the affected people have a reasonable expectation of an alternative or where lack of an alternative would meaningfully limit availability of a service or create unwarranted harmful impacts. Agencies should also seek to ensure that the opt-out mechanism itself does not impose discriminatory burdens on access to a government service. Agencies are not required to provide the ability to opt-out if the AI functionality is solely used for the prevention, detection, and investigation of fraud⁵² or cybersecurity incidents, or the conduct of a criminal investigation. Pursuant to the authority for waivers defined in Section 5(c)(ii), CAIOs are additionally permitted to waive this opt-out requirement if they can demonstrate that a human alternative would result in a service that is less fair (e.g., produces a disparate impact on protected classes) or if an opt-out would impose undue hardship on the agency.

d. Managing Risks in Federal Procurement of Artificial Intelligence

This section provides agencies with recommendations for responsible procurement of AI, supplementing an agency's required risk management practices above for rights-impacting AI and safety-impacting AI. In addition to these recommendations and consistent with section 7224(d) of the Advancing American AI Act and Section 10.1(d)(ii) of Executive Order 14110, OMB will also develop an initial means to ensure that Federal contracts for the acquisition of an AI system or service align with the guidance in this memorandum.

- i. **Aligning with the Law.** Agencies should ensure that procured AI is consistent with the Constitution and complies with all other applicable laws, regulations, and policies, including those addressing privacy, confidentiality, intellectual property, cybersecurity, human and civil rights, and civil liberties.
- ii. **Transparency and Performance Improvement.** Agencies should take steps to ensure transparency and adequate performance for their procured AI, including by:
 - A. obtaining adequate documentation to assess the AI's capabilities, such as through the use of model, data, and system cards;

⁵¹ See OMB [M-22-10](#) and supporting document "[Strategies for Reducing Administrative Burden in Public Benefit and Service Programs](#)."

⁵² Some uses of AI in these categories, such as the use of biometrics for identity verification, may be subject to requirements in other guidance that would necessitate an option to opt-out, and this memorandum does not replace, supersede, otherwise interfere with any such requirements.

- B. obtaining adequate documentation of known limitations of the AI and any guidelines on how the system is intended to be used;
 - C. obtaining adequate information about the provenance of the data used to train, fine-tune, or operate the AI;
 - D. regularly evaluating claims made by Federal contractors concerning both the effectiveness of their AI offerings as well as the risk management measures put in place, including by testing the AI in the particular environment where the agency expects to deploy the capability;
 - E. considering contracting provisions that incentivize the continuous improvement of procured AI; and
 - F. requiring sufficient post-award monitoring of the AI, where appropriate in the context of the product or service acquired.
- iii. **Promoting Competition in Procurement of AI.** Agencies should take appropriate steps to ensure that Federal AI procurement practices promote opportunities for competition among contractors and do not improperly entrench incumbents. Such steps may include promoting interoperability so that, for example, procured AI works across multiple cloud environments, and ensuring that vendors do not inappropriately favor their own products at the expense of competitors' offerings.
- iv. **Maximizing the Value of Data for AI.** In contracts for AI products and services, agencies should treat relevant data, as well as improvements to that data—such as cleaning and labeling—as a critical asset for their AI maturity. Agencies should take steps to ensure that their contracts retain for the Government sufficient rights to data and any improvements to that data so as to avoid vendor lock-in and facilitate the Government's continued design, development, testing, and operation of AI. Additionally, agencies should consider contracting provisions that protect Federal information used by vendors in the development and operation of AI products and services for the Federal Government, so that such data is protected from unauthorized disclosure and use and cannot be subsequently used to train or improve the functionality of the vendor's commercial offerings without express permission from the agency.
- v. **Overfitting to Known Test Data.** When testing AI using data that its developer may have access to—including test data that the agency has itself shared or released—agencies should ensure, as appropriate, that their AI developers or vendors are not directly relying on the test data to train their AI systems.⁵³
- vi. **Responsible Procurement of AI for Biometric Identification.** When procuring systems that use AI to identify individuals using biometric identifiers—e.g., faces, irises, fingerprints, or gait—agencies are encouraged to:
 - A. Assess and address the risks that the data used to train or operate the AI may not be lawfully collected or used, or else may not be sufficiently accurate to support reliable biometric identification. This includes the risks that the biometric information was collected without appropriate consent, was originally collected

⁵³ For instance, using validation data to train a model could lead the model to learn spurious correlations that make the model appear accurate in tests but harm the real-world performance of the AI system.

for another purpose, embeds unwanted bias, or was collected without validation of the included identities; and

- B. Request supporting documentation or test results to validate the accuracy, reliability, and validity of the AI's ability to match identities.

vii. **Responsibly Procuring Generative AI.** Agencies are encouraged to include risk management requirements in contracts for generative AI, and particularly for dual-use foundation models, including:

- A. requiring adequate testing and safeguards,
- B. requiring results of internal or external testing and evaluation, to include AI red-teaming against risks from generative AI, such as discriminatory, misleading, inflammatory, unsafe, or deceptive outputs;
- C. requiring that generative AI models have capabilities, as appropriate and technologically feasible, to reliably label or establish provenance for their content as generated or modified by AI; and
- D. incorporating relevant NIST standards, defined pursuant to Sections 4.1(a) and 10.1(d) of Executive Order 14110, as appropriate.

viii. **Assessing for Environmental Efficiency and Sustainability.** When procuring computationally intensive AI services, for example those that rely on dual-use foundation models, agencies should consider the environmental impact of those services, including whether the vendor has implemented methods to improve the efficiency and sustainability of such AI. This should include considering the carbon emissions and resource consumption from supporting data centers.

6. DEFINITIONS

The below definitions apply for the purposes of this memorandum.

Accessibility: The term “accessibility” has the meaning provided in Section 2(e) of Executive Order 14035.

Agency: The term “agency” has the meaning provided in 44 U.S.C. § 3502(1).

Algorithmic Discrimination: The term “algorithmic discrimination” has the meaning provided in Section 10(f) of Executive Order 14091 of February 16, 2023.

Artificial Intelligence (AI): The term “artificial intelligence” has the meaning provided in Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019,⁵⁴ which states that “the term ‘artificial intelligence’ includes the following”:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

⁵⁴ Pub. L. No. 115-232, § 238(g), <https://www.govinfo.gov/content/pkg/PLAW-115publ232/pdf/PLAW-115publ232.pdf>.

2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

For the purposes of this memorandum, the following technical context should guide interpretation of the definition above:

1. This definition of AI encompasses, but is not limited to, the AI technical subfields of machine learning (including deep learning as well as supervised, unsupervised, and semi-supervised approaches), reinforcement learning, transfer learning, and generative AI.
2. This definition of AI does not include robotic process automation or other systems whose behavior is defined only by human-defined rules or that learn solely by repeating an observed practice exactly as it was conducted.
3. For this definition, no system should be considered too simple to qualify as covered AI due to a lack of technical complexity (e.g., the smaller number of parameters in a model, the type of model, or the amount of data used for training purposes).
4. This definition includes systems that are fully autonomous, partially autonomous, and not autonomous, and it includes systems that operate both with and without human oversight.

AI and AI-Enabling Roles: The term “AI and AI-enabling roles” refers to individuals with positions and major duties whose contributions are important for successful and responsible AI outcomes. AI and AI-Enabling Roles include both technical and non-technical roles, such as data scientists, software engineers, data engineers, data governance specialists, statisticians, machine learning engineers, applied scientists, designers, economists, operations researchers, product managers, policy analysts, program managers, behavioral and social scientists, customer experience strategists, human resource specialists, contracting officials, managers, and attorneys.

AI Maturity: The term “AI maturity” refers to a Federal Government organization’s capacity to successfully and responsibly adopt AI into their operations and decision-making across the organization, manage its risks, and comply with relevant Federal law, regulation, and policy on AI.

AI Model: The term “AI model” has the meaning provided in Section 3(c) of Executive Order 14110.

AI Red-Teaming: The term “AI red-teaming” has the meaning provided for “AI red-teaming” in Section 3(d) of Executive Order 14110.

Applied Research: The term “applied research” refers to original investigation undertaken in order to acquire new knowledge to determine the means by which a specific practical aim or objective may be met.

Automation Bias: The term “automation bias” refers to the propensity for humans to inordinately favor suggestions from automated decision-making systems and to ignore or fail to seek out contradictory information made without automation.

Basic Research: The term “basic research” refers to experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts without a specific application towards processes or products in mind.

CFO Act Agency: The term “CFO Act Agency” refers to the agencies identified in 31 U.S.C. § 901(b).

Custom-Developed Code: The term “custom-developed code” has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Customer Experience: The term “customer experience” has the meaning established in Section 3(b) of Executive Order 14058.⁵⁵

Data Asset: The term “data asset” has the meaning provided in 44 U.S.C § 3502.

Dual-Use Foundation Model: The term “dual-use foundation model” has the meaning provided in Section 3(k) of Executive Order 14110.

Equity: The term “equity” has the meaning provided in Section 10(a) of Executive Order 14091.⁵⁶

Federal Information: The term “Federal information” has the meaning provided in OMB Circular A-130.

Generative AI: The term “generative AI” has the meaning provided in Section 3(p) of Executive Order 14110.

Intelligence Community: The term “intelligence community” has the meaning provided in 50 U.S.C. § 3003.

Model Weight: The term “model weight” has the meaning provided in Section 3(u) of Executive Order 14110.

⁵⁵ Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery To Rebuild Trust in Government*, <https://www.federalregister.gov/documents/2021/12/16/2021-27380/transforming-federal-customer-experience-and-service-delivery-to-rebuild-trust-in-government>.

⁵⁶ Executive Order 14091, *Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government*, <https://www.govinfo.gov/content/pkg/FR-2023-02-22/pdf/2023-03779.pdf>.

National Security System: The term “National Security System” has the meaning provided in 44 U.S.C. § 3552(b)(6).

Open Government Data Asset: The term “open government data asset” has the meaning provided in 44 U.S.C § 3502.

Open Source Software: The term “open source software” has the meaning provided in Appendix A of OMB Memorandum M-16-21.

Rights-Impacting AI:⁵⁷ The term “rights-impacting AI” refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant effect on that individual’s or entity’s:

1. Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance;
2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or
3. Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services.

Risks from the Use of AI: The term “risks from the use of AI” refers to risks related to efficacy, safety, equity, fairness, transparency, accountability, appropriateness, or lawfulness of a decision or action resulting from the use of AI to inform, influence, decide, or execute that decision or action. This includes such risks regardless of whether:

1. the AI merely informs the decision or action, partially automates it, or fully automates it;
2. there is or is not human oversight for the decision or action;
3. it is or is not easily apparent that a decision or action took place, such as when an AI application performs a background task or silently declines to take an action; or
4. the humans involved in making the decision or action or that are affected by it are or are not aware of how or to what extent the AI influenced or automated the decision or action.

While the particular forms of these risks continue to evolve, at least the following factors can create, contribute to, or exacerbate these risks:

1. AI outputs that are inaccurate or misleading;
2. AI outputs that are unreliable, ineffective, or not robust;
3. AI outputs that are discriminatory or have a discriminatory effect;
4. AI outputs that contribute to actions or decisions resulting in harmful or unsafe outcomes, including AI outputs that lower the barrier for people to take intentional and harmful actions;
5. AI being used for tasks to which it is poorly suited or being inappropriately repurposed in a context for which it was not intended;
6. AI being used in a context in which affected people have a reasonable expectation that a human is or should be primarily responsible for a decision or action; and

⁵⁷ Appendix I(2) of this memorandum lists AI applications that are presumed to be rights-impacting.

7. the adversarial evasion or manipulation of AI, such as an entity purposefully inducing AI to misclassify an input.

This definition applies to risks specifically arising from using AI and that affect the outcomes of decisions or actions. It does not include all risks associated with AI, such as risks related to the privacy, security, and confidentiality of the data used to train AI or used as inputs to AI models.

Safety-Impacting AI:⁵⁸ The term “safety-impacting AI” refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of:

1. Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms;
2. Climate or environment, including irreversible or significant environmental damage;
3. Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21⁵⁹ or any successor directive and the infrastructure for voting and protecting the integrity of elections; or,
4. Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

Significant Modification: The term “significant modification” refers to an update to an AI application or to the conditions or context in which it is used that meaningfully alters the AI’s impact on rights or safety, such as through changing its functionality, underlying structure, or performance such that prior evaluations, training, or documentation become misleading to users, overseers, or individuals affected by the system. This includes significantly changing the context, scope, or intended purpose in which the AI is used.

Underserved Communities: The term “underserved communities” has the meaning provided in Section 10(b) of Executive Order 14091.

⁵⁸ Appendix I(1) of this memorandum lists AI applications that are presumed to be safety-impacting.

⁵⁹ Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*, or successor directive, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

Appendix I: Purposes for Which AI is Presumed to be Safety-Impacting and Rights-Impacting

OMB has determined that the categories in this appendix in general meet the definition of safety-impacting AI or rights-impacting AI and are automatically *presumed* to be safety-impacting or rights-impacting. The following lists only identify a subset of uses of AI that impact rights and safety, and they do not represent an exhaustive list. Additionally, the presumption that a particular use of AI in the following lists will impact rights or safety can be waived by an agency's CAIO with adequate justification, pursuant to the processes outlined in Section 5.

1. Purposes That Are Presumed to Be Safety-Impacting. A use of AI is presumed to be safety-impacting if it is used or expected to be used, in real-world conditions, to control or significantly influence the outcomes of any of the following agency activities or decisions:

- a. Controlling the safety-critical functions within dams, emergency services, electrical grids, the generation or movement of energy, fire safety systems, food safety mechanisms, traffic control systems and other systems controlling physical transit, water and wastewater systems, or nuclear reactors, materials, and waste;
- b. Maintaining the integrity of elections and voting infrastructure;
- c. Controlling the physical movements of robots or robotic appendages within a workplace, school, housing, transportation, medical, or law enforcement setting;
- d. Applying kinetic force; delivering biological or chemical agents; or delivering potentially damaging electromagnetic impulses;
- e. Autonomously or semi-autonomously moving vehicles, whether on land, underground, at sea, in the air, or in space;
- f. Controlling the transport, safety, design, or development of hazardous chemicals or biological agents;
- g. Controlling industrial emissions and environmental impacts;
- h. Transporting or managing of industrial waste or other controlled pollutants;
- i. Designing, constructing, or testing of industrial equipment, systems, or structures that, if they failed, would pose a significant risk to safety;
- j. Carrying out the medically relevant functions of medical devices; providing medical diagnoses; determining medical treatments; providing medical or insurance health-risk assessments; providing drug-addiction risk assessments or determining access to medication; conducting risk assessments for suicide or other violence; detecting or preventing mental-health issues; flagging patients for interventions; allocating care in the context of public insurance; or controlling health-insurance costs and underwriting;
- k. Detecting the presence of dangerous weapons or a violent act;
- l. Choosing to summon first responders to an emergency;
- m. Controlling access to or security of government facilities; or
- n. Determining or carrying out enforcement actions pursuant to sanctions, trade restrictions, or other controls on exports, investments, or shipping.

2. Purposes That Are Presumed to Be Rights-Impacting. A use of AI is presumed to be rights-impacting if it is used or expected to be used, in real-world conditions, to control or significantly influence the outcomes of any of the following agency activities or decisions:

- a. Blocking, removing, hiding, or limiting the reach of protected speech;
- b. In law enforcement contexts, producing risk assessments about individuals; predicting criminal recidivism; predicting criminal offenders; identifying criminal suspects or predicting perpetrators' identities; predicting victims of crime; forecasting crime; detecting gunshots; tracking personal vehicles over time in public spaces, including license plate readers; conducting biometric identification (e.g., iris, facial, fingerprint, or gait matching); sketching faces; reconstructing faces based on genetic information; monitoring social media; monitoring prisons; forensically analyzing criminal evidence; conducting forensic genetics; conducting cyber intrusions in the course of an investigation; conducting physical location-monitoring or tracking of individuals; or making determinations related to sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention;
- c. Deciding or providing risk assessments related to immigration, asylum, or detention status; providing immigration-related risk assessments about individuals who intend to travel to, or have already entered, the U.S. or its territories; determining individuals' border access or access to Federal immigration related services through biometrics or through monitoring social media and other online activity; monitoring individuals' physical location for immigration and detention-related purposes; or forecasting the migration activity of individuals;
- d. Conducting biometric identification for one-to-many identification in publicly accessible spaces;
- e. Detecting or measuring emotions, thought, impairment, or deception in humans;
- f. Replicating a person's likeness or voice without express consent;
- g. In education contexts, detecting student cheating or plagiarism; influencing admissions processes; monitoring students online or in virtual-reality; projecting student progress or outcomes; recommending disciplinary interventions; determining access to educational resources or programs; determining eligibility for student aid or Federal education; or facilitating surveillance (whether online or in-person);
- h. Screening tenants; monitoring tenants in the context of public housing; providing valuations for homes; underwriting mortgages; or determining access to or terms of home insurance;
- i. Determining the terms or conditions of employment, including pre-employment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; performing time-on-task tracking; or conducting workplace surveillance or automated personnel management;
- j. Carrying out the medically relevant functions of medical devices; providing medical diagnoses; determining medical treatments; providing medical or insurance health-risk assessments; providing drug-addiction risk assessments or determining access to medication; conducting risk assessments for suicide or other violence; detecting or preventing mental-health issues; flagging patients for interventions; allocating care in the context of public insurance; or controlling health-insurance costs and underwriting;

- k. Allocating loans; determining financial-system access; credit scoring; determining who is subject to a financial audit; making insurance determinations and risk assessments; determining interest rates; or determining financial penalties (e.g., garnishing wages or withholding tax returns);
- l. Making decisions regarding access to, eligibility for, or revocation of critical government resources or services; allowing or denying access—through biometrics or other means (e.g., signature matching)—to IT systems for accessing services for benefits; detecting fraudulent use or attempted use of government services; assigning penalties in the context of government benefits;
- m. Translating between languages for the purpose of official communication to an individual where the responses are legally binding; providing live language interpretation or translation, without a competent interpreter or translator present, for an interaction that directly informs an agency decision or action; or
- n. Providing recommendations, decisions, or risk assessments about adoption matching, child protective actions, recommending child custody, whether a parent or guardian is suitable to gain or retain custody of a child, or protective actions for senior citizens or disabled persons.

Appendix II: Consolidated Table of Actions

Responsible Entity	Action	Section	Deadline
Each Agency	Designate an agency Chief AI Officer and notify OMB	3(a)(i)	60 days
Each CFO Act Agency	Convene agency AI Governance Board	3(a)(ii)	60 days
Each Agency	Submit to OMB and release publicly an agency plan to achieve consistency with this memorandum or a written determination that the agency does not use and does not anticipate using covered AI	3(a)(iii)	180 days and every two years thereafter until 2036
Each CFO Act Agency	Develop and release publicly an agency strategy for removing barriers to the use of AI and advancing agency AI maturity	4(a)(i)	365 days
Each Agency**	Publicly release an expanded AI use case inventory and report metrics on use cases not included in public inventories	3(a)(iv), 3(a)(v)	Annually
Each Agency*	Share and release AI code, models, and data assets, as appropriate	4(d)	Ongoing
Each Agency*	Stop using any safety-impacting or rights-impacting AI that is not in compliance with Section 5(c) and has not received an extension or waiver	5(a)(i)	December 1, 2024 (with extensions possible)
Each Agency*	Certify the ongoing validity of the waivers and determinations granted under Section 5(c) and 5(b) and publicly release a summary detailing each and its justification	5(a)(ii)	December 1, 2024 and annually thereafter
Each Agency*	Conduct periodic risk reviews of any safety-impacting and rights-impacting AI in use	5(c)(iv)(D)	At least annually and after significant modifications
Each Agency*	Report to OMB any determinations made under Section 5(b) or waivers granted under Section 5(c)	5(b); 5(c)(iii)	Ongoing, within 30 days of granting waiver

* Excluding elements of the Intelligence Community.

** Excluding elements of the Intelligence Community. The Department of Defense is exempt from the requirement to inventory individual use cases.

Open letter_ Why now is the time to act on US stat

Uploaded by: Katie Fry Hester

Position: FAV

[Store](#)[Log In](#)[All News](#)

12 Dec. 2024

OPINION

[Subscribe to Newsletters](#) →[Advertise with the IAPP](#) →[AI Governance](#)[Law & Regulation](#)

Open letter: Why now is the time to act on US state AI legislation

The Multistate AI Policymaker Working Group

Contributor

5 Minute Read

Artificial Intelligence holds the promise to help us solve big problems and enhance our efficiency, freeing us to focus on the things only humans can do. It has the potential to help us live longer, fuller lives and to revolutionize countless industries. AI is already assisting radiologists with detecting tumors earlier and identifying potential strokes and heart problems — enabling life-saving interventions.

We are only beginning to unlock AI's potential to improve our lives. However, to fully realize these benefits, we must address the associated risks and build consumer trust in the technology. As representatives closer to the people, state legislators have a unique vantage point on both the opportunities and challenges AI presents to our communities, businesses and government institutions.

Building trust, however, remains a challenge. According to the Pew Research Center Survey, 52% of people feel more concerned than excited about AI's potential, while only 10% of respondents are more excited than concerned. Concerns range from deepfake harms, unfairness and misinformation to the potential impact on critical infrastructure and loss of control as well as large consumption of electricity and water. Without safeguards, widespread adoption may stall. In fact, 67% of survey respondents believe government oversight of AI might not go far enough — and many fear it won't come quickly enough.

AI isn't the first technology to raise questions about trust — social media offers a valuable lesson. While it has helped connect the world, it has also been blamed for societal issues. Despite social media's prevalence, the last major federal data privacy law passed in 1998 — the Children's Online Privacy Protection Act. The U.S. remains one of the only G20 nations without a comprehensive data privacy law.

Recognizing the probability of congressional inaction, state legislators have come together to craft meaningful state-level AI laws. Despite different political affiliations, we share a commitment to pass meaningful legislation that ensures consumer safety and unlocks the full potential of AI for society. We are united around the following beliefs:

- The basis for AI state policy should be strong consumer data privacy laws that protect the privacy of individuals.
- Transparency is paramount and consumers have the right to know when a consequential decision is being made about their life by AI.
- Maintaining the human element is crucial. The ability of human oversight is needed for systems that make important decisions or that manage critical infrastructure.

A balanced approach grounded in bipartisan collaboration, transparency and accountability is essential to ensure AI serves the public good.

We have been working together since 2022 on common sense solutions. In 2023, 18 states and Puerto Rico adopted resolutions or enacted AI legislation. Thirty-one states, Puerto Rico and the Virgin Islands enacted AI legislation or resolutions and at least 27 states enacted deepfake legislation this year. Examples of the 2024 enactments include:

- Advisory councils and task forces to study the impact of AI in Colorado, Delaware, Indiana, North Carolina, Oregon, Pennsylvania, Puerto Rico, Tennessee, Texas, Virginia and West Virginia.
- In Colorado, Maryland and New York, requirements that state governments conduct impact assessments to ensure no state systems result in disparate impact.
- Grant programs to help states implement AI for specific uses in Connecticut, Maryland, Massachusetts, South Carolina and Washington.
- Comprehensive AI legislation in Colorado requiring developers and deployers of high-risk AI systems to use reasonable care to mitigate algorithmic discrimination and

disclose key information to consumers.

- Deepfake legislation addressing nonconsensual intimate images, sexually explicit or pornographic images of children or deceptive audio or visual media related to voting or candidates, and deceptive audio and visual media related to voting or candidates. This is in Alabama, Arizona, California, Colorado, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Minnesota, Mississippi, New Hampshire, New Mexico, New York, Oklahoma, Oregon, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia and Wisconsin.
- Transparency legislation, including data transparency, right to know when interacting with an AI system, and digital watermarking of content in California, Minnesota and Utah.

We are working together on legislation for 2025 and plan to release draft models of legislation by the beginning of January and gather feedback through virtual informational sessions.

While legislation may differ across states, we will collaborate to identify potential solutions and share resources. However, any model legislation crafted by specific lawmakers affiliated with our multistate group does not imply endorsement by any other member of the group or steering committee. Interested stakeholders can learn more about the [Multistate AI Policymaker Working Group](#) and how to submit feedback.

AI has the power to enhance the lives of all Americans. However, without thoughtful guardrails, there are risks of bias, inaccuracy and potential negative social impacts, as well as the possible introduction of new unforeseen dangers.

Now is the time to act — by working together, we can ensure AI serves the public good while protecting society from its dangers.

Signed by:

Name	State	Title
Scott Kawasaki	Alaska	State Senator
Shelley Hughes	Alaska	State Senator
Gail Pellerin	California	State Assemblymember
Jacqui Irwin	California	State Assemblymember
Rebecca Bauer-Kahan	California	State Assemblymember
Brianna Titon	Colorado	State Representative
Robert Rodriguez	Colorado	State Senator
Martin Looney	Connecticut	State Senator
Bob Duff	Connecticut	State Senator
Roland Lemar	Connecticut	State Representative
James Maroney	Connecticut	State Senator

Maria Horn	Connecticut	State Representative
Krista Griffith	Delaware	State Representative
Don Parsons	Georgia	State Representative
John Albers	Georgia	State Senator
Greggor Ilagan	Hawaii	State Representative
Kanani Souza	Hawaii	State Representative
Abdelnasser Rashid	Illinois	State Representative
Whitney Westerfield	Kentucky	State Senator
Amy D. Kuhn	Maine	State Representative
Daniel Sayre	Maine	State Representative
C.T. Wilson	Maryland	Delegate
Katie Fry Hester	Maryland	State Senator
Sara Love	Maryland	State Senator
Dawn D. Gile	Maryland	State Senator
Angelo Puppolo	Massachusetts	State Representative
Michael Moore	Massachusetts	State Senator
Tackey Chan	Massachusetts	State Representative
Kristin Bahner	Minnesota	State Representative
Steve Elkins	Minnesota	State Representative
Daniel Zolnikov	Montana	State Senator
Dina Neal	Nevada	State Senator
Angela Brennan	New Hampshire	State Representative
Christine Chandler	New Mexico	State Representative
Gail Chasey	New Mexico	State Representative
Harold Pope Jr.	New Mexico	State Senator
Debbie Sarinana	New Mexico	State Representative
Alex Bores	New York	State Assemblymember
Kristen Gonzalez	New York	State Senator
DeAndrea Salvador	North Carolina	State Senator
Munira Abdullahi	Ohio	State Representative
Arturo Alonso-Sandoval	Oklahoma	State Representative
Aaron Woods	Oregon	State Senator
Bob Merski	Pennsylvania	State Representative
Valerie Gaydos	Pennsylvania	State Representative
Napoleon Nelson	Pennsylvania	State Representative
Louis DiPalma	Rhode Island	State Senator
Liz Larson	South Dakota	State Senator

Heidi Campbell	Tennessee	State Senator
Giovanni Capriglione	Texas	State Representative
Brian Cina	Vermont	State Representative
Monique Priestley	Vermont	State Representative
Michelle Lopes Maldonado	Virginia	Delegate
Irene Shin	Virginia	Delegate
Lashrecse D. Aird	Virginia	Senator
Rodney Willett	Virginia	Delegate
Todd Pillion	Virginia	State Senator
Shelley Kloba	Washington	State Representative
Clyde Shavers	Washington	State Representative
Cindy Ryu	Washington	State Representative
Jarred Cannon	West Virginia	Delegate
Kelda Roys	Wisconsin	State Senator



This article is eligible for Continuing Professional Education credits. Please self-submit according to CPE policy guidelines.

Submit for CPEs

Interested in writing for us? Visit our Contributor Guidelines Page →

Related stories

Virginia Legislature passes AI bill, but unclear if governor will sign it

US District Court ruling resets 'pen register' litigation trend

Congressional committee kickstarts new federal privacy law dialogue

Notes from the IAPP Canada: Rick Mercer
to take Symposium stage

A view from DC: When Roosevelt fired an
FTC commissioner

About

The IAPP is a policy neutral, not-for-profit association founded in 2000 with a mission to define, promote and improve the professions of privacy, AI governance and digital responsibility globally.



Contact us



Press



Advertise



Become a member

The IAPP is the only place you'll find a comprehensive body of resources, knowledge and experts to help you navigate the complex landscape of today's data-driven world. We offer individual, corporate and group memberships, and all members have access to an extensive array of benefits.

[Sign up today](#)

[Privacy Notice](#)

[IAPP Cookie Notice](#)

[Conditions of Use](#)

[Refund Policy](#)

[Manage Cookies](#)

© 2025 IAPP. All rights reserved.

SB0936 Hester Testimony.pdf

Uploaded by: Katie Fry Hester

Position: FAV



THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Testimony in Support of SB936- Consumer Protection – High–Risk Artificial Intelligence – Developer and Deployer Requirements

February 27, 2025

Chair Beidle, Vice-Chair Hayes, and members of the Finance Committee.

Thank you for your consideration of SB936 - Consumer Protection for High-Risk Artificial Intelligence (AI) Systems. This legislation is essential to safeguarding Maryland residents as we navigate an era of rapid technological advancement. It establishes critical checks and balances to safeguard privacy, prevent discrimination, and ensure accountability in the deployment of high-risk AI systems.

Artificial intelligence is increasingly automating key aspects of hiring, employment, and financial decisions, often with little transparency or oversight. This has left consumers vulnerable to bias, errors, and privacy breaches. The consequences of unregulated AI are already evident across the country. In Michigan, the MiDAS unemployment claims system falsely accused over 34,000 individuals of fraud due to a lack of human oversight, with estimated damages approaching \$100 million.¹ In the private sector, Amazon was forced to abandon an AI-powered recruiting tool when it was found to systematically discriminate against female applicants.²

These cases are just the tip of the iceberg, highlighting the urgent need for regulation to prevent similar harm in Maryland. SB 936 accomplishes this by:

1. Establishing Developer Responsibilities:

- a. Exercise reasonable care to prevent known and foreseeable algorithmic discrimination.

¹ Robert N. Charette, "Michigan's Midas Unemployment System: Algorithm Alchemy Created Lead, Not Gold," IEEE Spectrum, June 24, 2021, <https://spectrum.ieee.org/michigans-midas-unemployment-system-algorithm-alchemy-that-created-lead-not-gold>.

² Jeffrey Dastin, "Insight - Amazon scraps secret AI recruiting tool that showed bias against women" Reuters, October 10, 2028 <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/>

- b. Provide deployers with necessary disclosures about the AI system's capabilities, limitations, and potential risks.
 - c. Make available documentation and information required for conducting impact assessments.
2. **Setting Obligations for AI Deployers:**
- a. Establish and maintain a risk management policy and program for each high-risk AI system in use.
 - b. Conduct impact assessments to evaluate the AI system's effects on consumers, particularly concerning algorithmic discrimination.
 - c. Inform consumers when a high-risk AI system is used in consequential decisions affecting them.
 - d. Provide mechanisms for consumers to correct information and appeal decisions made by AI systems.
3. **Enforcement and Consumer Rights:**
- a. The Maryland Attorney General is authorized to enforce compliance with the Act.
 - b. Consumers have the right to bring civil actions against deployers for violations, seeking remedies for harms caused by non-compliance.

For the past two years, I have served on the Steering Committee Multistate AI Policymaker Working Group, a bipartisan coalition of over 200 state lawmakers from more than 45 states dedicated to developing a shared understanding of emerging technologies and their policy implications. During the interim, the **Working Group facilitated discussions on AI consumer protection legislation**, with various models now being introduced and implemented across the country—including in [Colorado](#) (passed), [Virginia](#) (passed), [Connecticut](#) (pending), [New York](#) (pending), [Massachusetts](#) (pending), and [Texas](#) (pending).

This bill as drafted most closely follows the model established in Virginia's AI Consumer Protection Bill. However, I am committed to working with consumer rights and labor organizations to strengthen this bill from its current posture. As drafted, this bill has loopholes that would allow industry to not comply with large portions of it. I ask you to consider the amendments that advocacy groups are putting forth today.

Maryland has already demonstrated strong leadership in consumer protection with the passage of the Maryland Online Data Privacy Act and the Maryland Kids Code. Additionally, we passed SB 818, requiring state agencies to conduct Impact Assessments for new safety-impacting or rights-impacting systems that involve “high-risk” actions. SB 936 builds on this foundation, ensuring that AI-driven technologies operate fairly and transparently, safeguarding Marylanders from the dangers of bias and misuse.

AI is a powerful tool with incredible potential, but without the right safeguards, it can amplify bias, erode privacy, and undermine trust. Now is the time to act—before these risks become real

harms for Maryland residents. SB 936 positions our state as a leader in AI legislation, ensuring we remain ahead of the curve in consumer protection. For these reasons, I respectfully request a favorable report on SB 936.

Sincerely,

A handwritten signature in cursive script, appearing to read "Katie Fry Hester".

Senator Katie Fry Hester
Howard and Montgomery Counties

Testimony MD SB936_Feb. 25, 2025_CW.pdf

Uploaded by: Crystal Weise

Position: FWA



Good Afternoon, Senators of the Maryland General Assembly. My name is Crystal Weise. I am the Innovation Policy and Program Manager of the AFL-CIO Technology Institute (Tech Institute) and am also a Maryland resident. We are an independent, non-partisan organization affiliated with the AFL-CIO – a voluntary, democratic federation of 63 unions representing more than 15 million workers in all regions and sectors of the economy and public service. The AFL-CIO Technology Institute was launched to focus on the intersection of work and technology. It seeks to provide workers a voice in the technological developments sweeping the workplace and society, including artificial intelligence. We would like to express our position as favorable with amendments, and we are committed to working with the Senator to get the bill in the best posture possible to protect workers and consumers.

THE IMPACT OF UNREGULATED AI

The AI industry is rapidly transforming workplaces, leaving workers unprotected from [surveillance](#), privacy invasions, [discrimination](#), and erosion of labor rights. These technology systems are often linked to negative worker outcomes, including increased psychological stress, injury risk, scheduling and income instability, burnout, and turnover. In some cases, the implementation of data-driven systems impacts compensation structures in industries, for example, by "deskilling" work, depressing wages, eroding job security, or undermining royalty structures by threatening essential copyright and intellectual property protections. In other cases, these technologies can have a dramatic impact on other elements of job quality, including worker health and safety, professional discretion, [worker autonomy](#), [job satisfaction](#), and dignity. Beyond these effects, AI systems have shown algorithmic bias often resulting in discriminatory hiring practices and other hiring and compensation inequities. Employers [increasingly use](#) workplace AI systems for [key functions](#), such as hiring, scheduling, task assignment, performance evaluation, and even disciplining or terminating workers.

These immediate threats are real, and labor unions, public officials and civil society are leading the charge to fight back. But to proactively protect workers over the long-term, we must also strategize beyond these obstacles to prevent future ones through laws and regulations that shape and incentivize the technological development ecosystem.

Workers are [experts](#) in the use of technology. A lot can be learned by engaging them and their union representatives in the early stages of both the development of laws and the deployment of technology. Failure to involve workers meaningfully can lead to significant negative consequences especially if decisions about technology development and deployment are made that harm or ignore impacts on workers. Moreover, a technology ecosystem that fails to

incorporate workers into the development process risks slowing things down, stymieing innovation, and creating costly and negative outcomes.

FRAMEWORK FOR WORKER-CENTERED, UNION LED AI POLICY

We work with unions across the country on both federal and state-level policy. Labor has a broad framework for how technology should be governed and regulated. Legislation that protects end users (including workers) should include:

- Strong protections for both workers and consumers against discrimination and bias
- Transparency so workers and consumers know when and how companies use AI to make key decisions about them
- Broad definitions of covered systems to ensure accountability
- Ensure that consumer protections include workers and end users
- Include provisions for state governments as employers and deployers of AI
- Strong, loophole-free accountability and enforcement, including a private right of action
- Liability provisions to incentivize upstream technology development
- Mandatory consultation with workers and their unions when employers deploy AI

Putting these principles into practice is how we get to responsible and safe deployment of these technologies. We appreciate all the work that has been done by Senator Katie Fry Hester into developing guardrails for responsible AI policy. Several of these things are addressed in MD SB 936.

RECOMMENDATIONS

It's good to see that the bill addresses discrimination and potential harms to users with transparency requirements around disclosure, notification, and appeal processes. However, the legislation in its current state fails to protect workers and workplaces. Additionally, there are numerous loopholes that leave consumers and workers vulnerable to harm. We respectfully request that the bill be amended to strengthen the bill's ability to protect against the harms of AI.

Strengthen Worker Protections

The existing definition of "consumer" excludes workers in employment capacity (pg. 4, 14–47A–01). Furthermore, the bill lacks mechanisms for public and worker input in AI governance.

Solidify Definitions

A number of definitions should be strengthened to remove unnecessary exclusions and loopholes that undermine accountability for developers and deployers of AI. For example, the bill excludes certain technologies, including chatbots that can harm users. Additionally, the definition of "substantial factor" as the "principal factor" leaves open the opportunity for companies to evade the law by assigning a human to rubber-stamp AI decisions.

Close Loopholes

The impact assessment does not require an independent 3rd party independent auditor, allowing for self-policing. Furthermore, exemptions for anything a company considers “confidential” or a “trade secret” allow companies to skirt disclosure requirements. There are also numerous carveouts including for some insurance and healthcare uses that leave workers and consumers exposed to harms.

Inadequate Enforcement Mechanisms

Affirmative defenses and rebuttable presumptions undermine accountability and enforcement of the bill’s provisions, allowing companies to ignore or circumvent regulations.

In order to address these issues and others, we recommend the following amendments:

On pg. 3, under (D)(3), insert:

(i) “INCLUDING ANY DECISION MADE BY AN EMPLOYER THAT AFFECTS WAGES, BENEFITS, OTHER COMPENSATION, HOURS, SCHEDULE, PERFORMANCE EVALUATION, HIRING, RECRUITMENT, DISCIPLINE, PROMOTION, TERMINATION, DUTIES, ASSIGNMENT OF WORK, ACCESS TO WORK OPPORTUNITIES, PRODUCTIVITY REQUIREMENTS, WORKPLACE HEALTH AND SAFETY, OR OTHER TERMS OR CONDITIONS OF EMPLOYMENT”

On pg. 4, (E)(1) should read:

“CONSUMER” MEANS AN INDIVIDUAL WHO:
(I) IS A RESIDENT OF THE STATE
(II) IS AN EMPLOYEE AS DEFINED IN § 3-1001 OF THE LABOR AND EMPLOYMENT ARTICLE
(III) IS EMPLOYED BY A BUSINESS IN THE STATE

On pg. 4, **strike lines 7-8**

On pg. 5, **replace lines 4-7 with:**

“HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM MEANS AN ARTIFICIAL INTELLIGENCE SYSTEM THAT, WHEN DEPLOYED, MAKES, OR IS A SUBSTANTIAL FACTOR IN MAKING, A CONSEQUENTIAL DECISION.”

On pg. 5, **strike lines 13-14**

On pg. 5, **strike lines 17-18**

On pg. 5, **strike line 25**

On pg. 5, **strike line 27**

On pg. 5, **strike line 28**

On pg. 6, **strike lines 10-14**

On pg. 7, **strike lines 1-16**

On pg. 7, under (M)(1), include "GOVERNMENTAL UNIT" to read:

"Person" MEANS AN INDIVIDUAL, AN ASSOCIATION, A COOPERATIVE, A CORPORATION, A LIMITED LIABILITY COMPANY, A PARTNERSHIP, A TRUST, A JOINT VENTURE, **A GOVERNMENTAL UNIT**, OR ANY OTHER LEGAL OR COMMERCIAL ENTITY AND ANY SUCCESSOR, REPRESENTATIVE, AGENCY, OR INSTRUMENTALITY THEREOF.

On pg. 7, **strike line 21**

On pg. 8, **strike lines 12-31 (section 14-47A-02)**

On pg. 9, **strike lines 1-8**

On pg. 9, **strike lines 14-18**

On pg. 12, **strike lines 1-14**

On pg. 12, **strike lines 15-23**

On pg. 13, **strike lines 26-30**

On pg. 13, under section 14-47A-04, insert:

“(A) THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED

(B) “IMPACT ASSESSMENT” MEANS AN IMPARTIAL EVALUATION BY AN INDEPENDENT AUDITOR

(C)(1)“INDEPENDENT AUDITOR” MEANS A PERSON OR THIRD-PARTY ENTITY THAT CONDUCTS AN IMPACT ASSESSMENT OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM TASKED WITH MAKING A CONSEQUENTIAL DECISION AS DEFINED IN 14-47A-01(D)

(2) “INDEPENDENT AUDITOR” DOES NOT INCLUDE

(I) A PERSON CURRENTLY OR AT ANY POINT IN THE 5 YEARS PRECEDING THE IMPACT ASSESSMENT

(a) ARE OR WERE INVOLVED IN USING, DEVELOPING, OFFERING, LICENSING, OR DEPLOYING THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM;

(b) HAVE OR HAD AN EMPLOYMENT RELATIONSHIP WITH A DEVELOPER OR DEPLOYER THAT USES, OFFERS, OR LICENSES THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM; OR

(c) HAVE OR HAD A DIRECT FINANCIAL INTEREST OR MATERIAL INDIRECT FINANCIAL INTEREST IN A DEVELOPER OR DEPLOYER THAT USES, OFFERS, OR LICENSES THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM

On pg. 14, **strike lines 32-34**

On pg. 15, **strike lines 1-13**

On pg. 17, replace (3) with:

“(3) PRIOR TO DEPLOYMENT OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM, OR SIX MONTHS AFTER DEPLOYMENT, AND AT LEAST EIGHTEEN MONTHS THEREAFTER FOR EACH CALENDAR YEAR A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM IS IN USE AFTER THE FIRST POST-DEPLOYMENT AUDIT, EVERY DEVELOPER OR DEPLOYER OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM SHALL CONDUCT AT LEAST ONE THIRD-PARTY IMPACT ASSESSMENT TO ENSURE THAT THE PRODUCT DOES NOT PRODUCE ALGORITHMIC DISCRIMINATION AS DEFINED IN 14-47A-01(B)(1)”

On pg. 17, **replace “(3)” with “(4)”**

In that same line, replace “3 YEARS” with “5 YEARS”

On pg. 17, **replace “(4)” with “(5)”**

On pg. 19, in line 6, **strike “UNLESS PROVIDING THIS OPPORTUNITY”**

On pg. 19, **strike lines 7-9**

On pg. 21, in line 23, **replace “MAY” with “SHALL”**

To truly protect workers and consumers, strong protections against the harms of AI and a role for worker voice in the implementation of the technology are essential strategies. Maryland’s workers deserve comprehensive and robust protections for consumers and workers from AI.

SB 936 - AI.pdf

Uploaded by: Denise Riley

Position: FWA

On behalf of AFT Maryland's over 18,000 members, I appreciate the opportunity to provide testimony on SB 936.

AFT Maryland appreciates the aims of this bill. In the absence of coherent federal policy regulating artificial intelligence, it is important that the states step up and protect workers and consumers from foreseeable AI harms. Automated decision-making systems impact workers and consumers statewide, and regulating these AI models is a deserving task for the legislature. With SB 936, we are concerned that the current language creates loopholes which will allow companies to easily evade the disclosure requirements contained within the bill.

If left unaddressed, these loopholes will render nearly all the protections of SB 936 entirely ineffective. While we would love to be able to support state legislation that protects Marylanders from algorithm discrimination, AFT Maryland opposes this bill in its current form and implores you to work to address the bill's weaknesses.

The definition of consumer excludes workers and those traditionally considered to be consumers:

We tend to think of consumers as actors within a commercial context-- buyers of goods or services. This bill is written to define consumers in a way that "does not include an individual acting in a commercial or employment context." Since consumers are the only individuals receiving protection in this bill, it is strange that the legislation is written to define consumers as excluding those traditionally thought of as engaging in commerce. In addition, this bill makes repeated reference to employment decisions throughout the text, but definitionally excludes workers with this "employment context" carve out.

Marylanders deserve protection from automated decision making in the workplace. Using a definition of "consumer" which bears little relation to the commonly understood definition of consumer is shameful and needs to immediately be addressed. When legislators define words to have definitions that run contrary to their commonly understood meanings, confidence in our democracy suffers. These protections need to apply to consumers (i.e. Marylanders who "act in a commercial context" by buying goods and services). It also must apply to workers and others in an employment context.

There are loopholes in this bill that will allow companies to easily skirt consumer protections:

Again, AFT Maryland appreciates the stated aims of this bill, which seeks to prevent Marylanders from suffering discrimination at the hands of automated decision-making systems. As currently written, this bill simply will not accomplish those aims. The bill suffers from multiple loopholes and poor definitions which, unless addressed, will foreseeably allow AI companies to skirt the protections in this bill.

1) The protections in this bill apply only when an automated decision system is a "substantial factor" in making a "consequential decision." Similar bills have been introduced across the country, and "substantial factor" was swapped in for "controlling factor" after it was reported that these bills were based on model language written by lobbyists for a company called Workday, which makes automated decision-making systems.¹ When activists pushed back on "controlling factor" as a definition which would exclude any real-life automated decision system from oversight, "substantial factor" began to be used to address the concerns of civil rights groups. In SB 936, "substantial factor" has been effectively redefined back to controlling factor, by defining it as something which is the "principal basis for making a consequential decision." We're back to where Workday and the tech companies want this bill- written to prevent it from ever being applied to their software. By simply advertising (or putting into their terms of service) that their program cannot be the principal basis for making a consequential decision, companies can evade this law.

¹ <https://therecord.media/human-resources-artificial-intelligence-state-legislation-workday>

2) For companies that don't want to evade the requirements of this bill through fine print alone, the legislation offers three additional carve outs for trade secrets and confidential and proprietary information. There is nothing in this legislation which enables any instrumentality of the state to evaluate asserted exemptions for trade secrets, confidentiality, or proprietary information. Manufacturers of the automated decision-making systems covered by this bill will likely over-assert these exemptions.

Marylanders deserve legislation that cannot be defeated by fine print. Protecting the citizens of this state from automated decision-making systems should not be left to lobbyists from companies that sell those systems. We deserve to have legislative definitions of terms that resemble the actual and common definitions of those words, not definitions which contort language itself. Marylanders deserve to have bills written to protect them, not written by lobbyists seeking to hoodwink them.

I hope the legislature will address the serious issues plaguing this bill.

SB0936 - FWA - MMBBA - Gough - REV.pdf

Uploaded by: DENNIS RASMUSSEN

Position: FWA



Testimony offered on behalf of:
MARYLAND MORTGAGE BANKERS & BROKERS ASSOCIATION, INC.

IN SUPPORT, WITH AMENDMENT TO:
**SB0936 – Consumer Protection – High-Risk Artificial Intelligence –
Developer and Deployer Requirements**

Senate Finance Committee
Hearing: 2/27/2025 at 1:00 PM

The Maryland Mortgage Bankers and Brokers Association (MMBBA) acknowledges the intent of **SB0936**, which aims to protect consumers from potential harm associated with high-risk artificial intelligence (AI) systems. However, **we advocate for exemptions to address the harm the bill would have on the residential mortgage banking industry in Maryland.**

The mortgage banking industry should be exempt from SB0936 because the use of AI is already regulated under an existing comprehensive federal regulatory framework. Conversely, the Mortgage Bankers Association (MBA) has expressed concerns that a patchwork of state laws and federal regulations could lead to higher compliance costs and disrupt access to credit for consumers. The MBA advocates for uniform federal legislation to address AI-related issues, suggesting that state-level regulations may be redundant and potentially conflicting.¹

Federal agencies have already established guidelines and rules to ensure the responsible deployment of AI in mortgage lending. Financial institutions are subject to routine on-site examination by prudential regulators and examiners who ensure compliance with laws and regulations, including consumer protection and anti-discrimination laws. Regulators have consistently emphasized that financial institutions must identify, measure, monitor, and manage risks arising from the use of AI. “Regardless of how AI is used in the activities of a financial institution, the institution is responsible for adherence to applicable laws and regulations.”²

Regulatory and supervisory oversight includes the review and assessment of institutions’ practices for identifying, monitoring, and controlling the risk of discrimination or bias in AI systems.

¹ Mortgage Bankers Association, AI in the Mortgage Industry (Nov. 2024), available [here](#).

² U.S. Department of Treasury, Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector (March 2024), available [here](#).

- Equal Credit Opportunity Act (ECOA): ECOA, and its implementing regulation, Regulation B, promulgated by the Consumer Financial Protection Bureau (CFPB) prohibits lenders from using AI to discriminate against applicants during a credit transaction based on race, color, religion, national origin, sex (including sexual orientation and gender identity), marital status, age, whether all or part of the applicant's income derives from any public assistance program, or the applicant's good faith exercise of any right under the Consumer Credit Protection Act. Lenders have necessarily used algorithms and AI for many years to promptly complete a consumer's request for the extension of credit. In instances where that credit is denied, a lender must provide notice that is specific and indicate the principal reasons for the adverse action. Under CFPB Circular 2022-03, creditors cannot merely rely on the output of an AI as a reason to deny credit and must disclose a specific reason for the denial. ECOA is enforced by the CFPB and can be enforced by the Maryland Attorney General.
- Fair Housing Act (FHA): The FHA prohibits discrimination in all aspects of residential real estate-related transactions based on race, color, religion, sex (including sexual orientation and gender identity), national origin, disability, and familial status. The FHA is enforced by the Department of Justice.
- Fair Credit Reporting Act (FCRA): FCRA requires creditors to provide an adverse action notice, like ECOA, if their decision is based on information contained in a consumer credit report. Additionally, FCRA allows consumers to dispute the completeness or accuracy of information in their credit report and requires that a credit reporting agency investigate this claim.

The systems and models developed and authorized by the Government-Sponsored Enterprises (GSEs) and federal agencies are developed and utilized within this regulatory framework, ensuring consumer protection and fairness. Given existing federal oversight, exempting the mortgage banking industry from **SB0936** would allow the industry to continue its operations under the established federal framework. At a minimum, we recommend that AI systems developed or authorized by GSEs or federal agencies, such as Automated Underwriting Systems (AUS) and Credit Scoring Models, be exempt from the provisions of **SB0936**. These systems are integral to the mortgage lending process, providing efficiency and consistency in credit risk assessment. They operate under stringent federal regulations and oversight, ensuring their reliability and fairness. Credit Scoring Models are essential tools in evaluating borrowers' creditworthiness and are developed following federal guidelines to prevent discrimination and ensure accuracy.

While we understand the concerns of **SB0936** in safeguarding consumers from potential risks associated with high-risk AI systems, we believe that the residential mortgage banking industry operates under established federal regulations that already address the concerns contemplated by this bill. Therefore, we respectfully

2/24/2025

SB0936

request that **SB0936** include explicit exemptions for the mortgage banking industry or, at a minimum, an exemption for AI models that have been developed or authorized by the GSEs or federal government, including credit scoring models, to avoid raising the cost of providing credit to Maryland residents. By incorporating these exemptions, **SB0936** can achieve its consumer protection goals without imposing unnecessary constraints.

For these reasons, the MMBBA **supports, with an amendment to SB0936.**

Respectfully submitted,

Tim Gough

Timothy J. Gough

MMBBA Legislative Committee Member

tgough@baycapitalmortgage.com – (410) 320-0852

SB 936 - Consumer Protection - High-Risk Artificial

Uploaded by: Donna Edwards

Position: FWA



MARYLAND STATE & D.C. AFL-CIO

AFFILIATED WITH NATIONAL AFL-CIO

7 School Street • Annapolis, Maryland 21401-2096

Balto. (410) 269-1940 • Fax (410) 280-2956

President

Donna S. Edwards

Secretary-Treasurer

Gerald W. Jackson

SB 936 - Consumer Protection - High-Risk Artificial Intelligence - Developer and Deployer Requirements
Senate Finance Committee
February 27, 2025

SUPPORT with AMENDMENTS

Donna S. Edwards
President
Maryland State and DC AFL-CIO

Madame Chair and members of the Committee, thank you for the opportunity to submit testimony in support of SB 936 if amended. My name is Donna S. Edwards, and I am the President of the Maryland State and District of Columbia AFL-CIO. On behalf of Maryland's 300,000 union members, I offer the following comments.

SB 936 aims to create guardrails around the development and deployment of high-risk artificial intelligence (AI) systems to ensure fair and equitable decision-making. We support the provisions of the bill that enhance transparency as it provides individuals with a deeper understanding of the impacts of these types of systems. We applaud the sponsor's work to mitigate associated risks.

Strong AI legislation should include:

- Strong protections for both workers and consumers against discrimination and bias
- Transparency so workers and consumers know when and how companies use AI to make key decisions about them
- Broad definitions of covered systems to ensure accountability
- Ensure that consumer protections include workers and end users
- Include provisions for state governments as employers and deployers of AI
- Strong, loophole-free accountability and enforcement
- Liability provisions to incentivize upstream technology development
- Mandatory consultation with workers and their unions when employers deploy AI

However, SB 936 has several missing provisions including adequate worker protections, comprehensive definitions, measures to close loopholes that undermine accountability, and strong enforcement mechanisms.

As the AI industry continues to evolve, it is critical that we implement strong protections that close these gaps and do not allow companies to opt out of complying with the law. To address these concerns, we propose the following amendments:

On pg. 3, under (D)(3), insert:

(i) “INCLUDING ANY DECISION MADE BY AN EMPLOYER THAT AFFECTS WAGES, BENEFITS, OTHER COMPENSATION, HOURS, SCHEDULE, PERFORMANCE EVALUATION, HIRING, RECRUITMENT, DISCIPLINE, PROMOTION, TERMINATION, DUTIES, ASSIGNMENT OF WORK, ACCESS TO WORK OPPORTUNITIES, PRODUCTIVITY REQUIREMENTS, WORKPLACE HEALTH AND SAFETY, OR OTHER TERMS OR CONDITIONS OF EMPLOYMENT”

On pg. 4, (E)(1) should read:

“CONSUMER” MEANS AN INDIVIDUAL WHO:

(I) IS A RESIDENT OF THE STATE

(II) IS AN EMPLOYEE AS DEFINED IN § 3-1001 OF THE LABOR AND EMPLOYMENT ARTICLE

(III) IS EMPLOYED BY A BUSINESS IN THE STATE

On pg. 4, **strike lines 7-8**

On pg. 5, **replace lines 4-7 with:**

“HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM MEANS AN ARTIFICIAL INTELLIGENCE SYSTEM THAT, WHEN DEPLOYED, MAKES, OR IS A SUBSTANTIAL FACTOR IN MAKING, A CONSEQUENTIAL DECISION.”

On pg. 5, **strike lines 13-14**

On pg. 5, **strike lines 17-18**

On pg. 5, **strike line 25**

On pg. 5, **strike line 27**

On pg. 5, **strike line 28**

On pg. 6, **strike lines 10-14**

On pg. 7, **strike lines 1-16**

On pg. 7, under (M)(1), include “GOVERNMENTAL UNIT” to read:

“Person” MEANS AN INDIVIDUAL, AN ASSOCIATION, A COOPERATIVE, A CORPORATION, A LIMITED LIABILITY COMPANY, A PARTNERSHIP, A TRUST, A JOINT VENTURE, **A GOVERNMENTAL UNIT**, OR ANY OTHER LEGAL OR COMMERCIAL ENTITY AND ANY SUCCESSOR, REPRESENTATIVE, AGENCY, OR INSTRUMENTALITY THEREOF.

On pg. 7, **strike line 21**

On pg. 8, **strike lines 12-31 (section 14-47A-02)**

On pg. 9, **strike lines 1-8**

On pg. 9, **strike lines 14-18**

On pg. 12, **strike lines 1-14**

On pg. 12, **strike lines 15-23**

On pg. 13, **strike lines 26-30**

On pg. 13, under section 14-47A-04, insert:

“(A) THE FOLLOWING WORDS HAVE THE MEANINGS INDICATED

(B) “IMPACT ASSESSMENT” MEANS AN IMPARTIAL EVALUATION BY AN INDEPENDENT AUDITOR

(C)(1)“INDEPENDENT AUDITOR” MEANS A PERSON OR THIRD-PARTY ENTITY THAT CONDUCTS AN IMPACT ASSESSMENT OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM TASKED WITH MAKING A CONSEQUENTIAL DECISION AS DEFINED IN 14-47A-01(D)

(2) “INDEPENDENT AUDITOR” DOES NOT INCLUDE

(I) A PERSON CURRENTLY OR AT ANY POINT IN THE 5 YEARS PRECEDING THE IMPACT ASSESSMENT

(a) ARE OR WERE INVOLVED IN USING, DEVELOPING, OFFERING, LICENSING, OR DEPLOYING THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM;

(b) HAVE OR HAD AN EMPLOYMENT RELATIONSHIP WITH A DEVELOPER OR DEPLOYER THAT USES, OFFERS, OR LICENSES THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM; OR

(c) HAVE OR HAD A DIRECT FINANCIAL INTEREST OR MATERIAL INDIRECT FINANCIAL INTEREST IN A DEVELOPER OR DEPLOYER THAT USES, OFFERS, OR LICENSES THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM

On pg. 14, **strike lines 32-34**

On pg. 15, **strike lines 1-13**

On pg. 17, replace (3) with:

“(3) PRIOR TO DEPLOYMENT OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM, OR SIX MONTHS AFTER DEPLOYMENT, AND AT LEAST EIGHTEEN MONTHS THEREAFTER FOR EACH CALENDAR YEAR A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM IS IN USE AFTER THE FIRST POST-DEPLOYMENT AUDIT, EVERY DEVELOPER OR DEPLOYER OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM SHALL CONDUCT AT LEAST ONE THIRD-PARTY IMPACT ASSESSMENT TO ENSURE THAT THE PRODUCT DOES NOT PRODUCE ALGORITHMIC DISCRIMINATION AS DEFINED IN 14-47A-01(B)(1)”

On pg. 17, replace “(3)” with “(4)”

In that same line, replace “3 YEARS” with “5 YEARS”

On pg. 17, replace “(4)” with “(5)”

On pg. 19, in line 6, **strike “UNLESS PROVIDING THIS OPPORTUNITY”**

On pg. 19, **strike lines 7-9**

On pg. 21, in line 23, **replace “MAY” with “SHALL”**

MTC Policy Statement on AI.pdf

Uploaded by: Drew Vetter

Position: FWA



Maryland Tech Council

Artificial Intelligence Policy Statement

The continued development and adoption of artificial intelligence (AI) has the potential to transform many aspects of society and our daily lives, from how we interact online to education, e-commerce, healthcare delivery, finance, and many other applications. The Maryland Tech Council (MTC) is optimistic about the promise of AI to be a force of good and positive societal change. However, MTC is clear that adoption of AI carries risks that must be considered by innovators and policymakers. Elected leaders, regulators, and the private sector must work together to ensure that the use of AI is safe, ethical, responsible, and trustworthy. We must protect against unintended harms such as bias and disproportionate impact on marginalized communities.

The promise and risks inherent in the adoption of AI has policymakers at the federal, state, and local levels of government considering laws, regulations, and other measures to examine the complex issues presented above. As such, the MTC has developed a set of factors to be considered by policymakers and regulators when considering new efforts to govern the use and adoption of AI.

- Ensure broad representation of industry sectors on new commissions and boards. There are different use cases and impacts depending on sector, be it healthcare, finance, education, etc. To the extent these impacts are being regulated, policymakers should bring subject matter experts and stakeholders into the discussion.
- Policymakers are considering various new assessments or certifications of AI tools. Any new requirements must be clear and specific. Overly broad requirements make it difficult for industry to evaluate impact and comply with. Consider using risk assessment standards and practices that already exist, such as the NIST AI Risk Management Framework.
- Be mindful in defining new terms, ensuring that there are not multiple definitions of the same or similar terms and that there is not conflict with Federal definitions. Strive for consistency with other states so as not to have a patchwork of laws from state to state. Avoid creating overly broad discretion of terms that subject companies to liability such as the definition of a harmful or high-risk action or impact.
- Special deliberation should occur around the challenges and opportunities presented by Open Source AI. Open Source AI is critical to the democratization of AI technologies beyond a few massive technology providers. Yet, Open Source AI systems must be rigorously reviewed and assessed from a security perspective. Policy leaders should consult with the private sectors to ensure an understanding of the benefits of Open Source AI while providing reasonable expectations to securing these platforms.

- The implications on the workforce must be incorporated into AI policy discussions. A majority of companies lack enough skilled employees for future growth. AI developers, learning institutions, training programs, and prospective workers must coordinate to ensure we have an AI-ready workforce.
- Consideration should always be given to smaller and medium sized local businesses when new AI laws or regulations are being adopted. Far too often, these laws are considered with only the largest technology companies in mind, when smaller and locally based businesses are impacted just the same. Often, these smaller companies lack the resources to quickly adapt and comply with complex new laws.
- Enforcement mechanisms must be calibrated to be consistent with the level of risk that AI solutions present, especially in cases where there is a new risk created by AI that is not already addressed. Liability and enforcement standards should be thoughtful and proportionate, with an emphasis on compliance over being punitive. Distinctions between 3rd party services, technology providers, and end-users should be accounted for, as well as recognition of good faith efforts to develop technology that evolves and improves over time.

SB0936_FWA_MTC_Con. Prot. - High-Risk AI - Develop

Uploaded by: Drew Vetter

Position: FWA

Senate Finance Committee

February 27, 2025

Senate Bill 936 – *Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements*

SUPPORT WITH AMENDMENT

The Maryland Tech Council (MTC), with over 800 members, is the State’s largest association of technology companies. Our vision is to propel Maryland to be the country's number one innovation economy for life sciences and technology. MTC brings the State’s life sciences and technology communities into a single, united organization that empowers members to achieve their goals through advocacy, networking, and education. On behalf of MTC, we submit this letter of support with amendment for Senate Bill 936.

MTC supports the development of a sensible framework for the regulation of high-risk artificial intelligence. We believe that elected leaders, regulators, and the private sector must work together to ensure that the use of AI is safe, ethical, responsible, and trustworthy and that we must protect against unintended harm, such as bias and disproportionate impact on marginalized communities. In 2024, the MTC developed an “Artificial Intelligence Policy Statement” that contains a set of factors to be considered by policymakers and regulators when deliberating new efforts to govern the use of AI. These factors are the basis for how MTC evaluates AI policies and regulations.

To that end, we appreciate the sponsor’s focus on “high-risk” use cases of AI when used to make a “consequential decision.” Additionally, we appreciate this legislation’s focus on preventing algorithmic discrimination. Numerous MTC member companies have reviewed this legislation and have various suggestions to improve the bill and strike the proper balance between strong consumer protections, practicality of compliance, and proportionate enforcement. MTC members have shared the following feedback on the bill:

14-47A-01 - Definitions

- “Generative Artificial Intelligence” definition should be changed to clarify that it applies to an “Artificial Intelligence SYSTEM that is capable of...” This is consistent with other state definitions, including the AI bill just passed in Virginia.
- “Intentional and Substantial Modification” should be expanded to include additional clarity around customization by deployers.
- Consider adding definitions of the following terms:
 - "MACHINE LEARNING" MEANS THE DEVELOPMENT OF ALGORITHMS TO BUILD DATA-DERIVED STATISTICAL MODELS THAT ARE CAPABLE OF DRAWING INFERENCES FROM PREVIOUSLY UNSEEN DATA WITHOUT EXPLICIT HUMAN INSTRUCTION.
 - "RED-TEAMING" MEANS ADVERSARIAL TESTING TO IDENTIFY THE POTENTIAL ADVERSE BEHAVIORS OR OUTCOMES OF AN ARTIFICIAL INTELLIGENCE SYSTEM, IDENTIFY HOW SUCH BEHAVIORS OR OUTCOMES OCCUR, AND STRESS TEST THE SAFEGUARDS AGAINST SUCH BEHAVIORS OR OUTCOMES.
 - "TRADE SECRET" HAS THE 15 MEANING STATED IN § 11-1201 OF THIS ARTICLE.
- Under (K)(2)(II), language should be added that a “High-Risk Artificial Intelligence System” includes exempting “Clinical and Pre-Clinical Research and Development.” This would encourage innovation and protect companies that are using AI in R&D activities, which is common in life sciences and Fintech.

14-47A-03 – Developer Obligations

- The Effective Date should be changed so that there are at least 18 months from the passage for implementation; the current implementation deadline of February 1, 2026, is too short and will hinder compliance.
- We are concerned that smaller companies will have difficulty complying with this section (as well as 14-47A-04). We request consideration of exempting small businesses with fewer than 50 employees or \$5 million in revenue from full documentation and assessment requirements or to offer a simplified compliance model. We would also recommend a 2-year grace period for start-up companies. Making such provisions for small businesses will allow small tech firms to grow without overly burdensome compliance overhead.
- In (A)(1) the “reasonable care” standard should be changed to “Industry Standard Means.” This will provide more certainty around compliance.
- The bill should recognize that multiple developers may be involved, so disclosures should be made to other developers as well as deployers, which is inconsistently applied throughout the bill. Further, the addition of this language will fairly distribute obligations.

WHERE MULTIPLE DEVELOPERS DIRECTLY CONTRIBUTE TO THE DEVELOPMENT OF A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM, EACH DEVELOPER SHALL BE SUBJECT TO THE OBLIGATIONS AND OPERATING STANDARDS APPLICABLE TO DEVELOPERS PURSUANT TO THIS SECTION SOLELY WITH RESPECT TO ITS ACTIVITIES CONTRIBUTING TO THE DEVELOPMENT OF THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM

- More clarity around treatment of synthetic data, especially around marking requirements where certain pieces may not be technologically feasible.

14-47A-04 – Deployer Obligations

- Clarity should be added for deployer obligations that they apply to using a high-risk artificial intelligence system to make a consequential decision – in both the case of risk management policies and for completing impact assessments.
- Include the same provisions for small businesses as referenced in bullet #2 in 14-47A-03 above.
- Recognition of compliance with risk management frameworks already in place.

- HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS THAT ARE IN CONFORMITY WITH THE LATEST VERSION OF THE ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK PUBLISHED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, STANDARD ISO/IEC 42001 OF THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, OR ANOTHER NATIONALLY OR INTERNATIONALLY RECOGNIZED RISK MANAGEMENT FRAMEWORK FOR ARTIFICIAL INTELLIGENCE SYSTEMS, OR PARTS THEREOF, SHALL BE PRESUMED TO BE IN CONFORMITY WITH RELATED REQUIREMENTS SET OUT IN THIS SECTION AND IN ASSOCIATED REGULATIONS. IF A DEPLOYER COMPLETES AN IMPACT ASSESSMENT FOR THE PURPOSE OF COMPLYING WITH ANOTHER APPLICABLE LAW OR REGULATION, SUCH IMPACT ASSESSMENT SHALL BE DEEMED TO SATISFY THE REQUIREMENTS ESTABLISHED IN THIS SUBSECTION IF SUCH IMPACT ASSESSMENT IS REASONABLY SIMILAR IN SCOPE AND EFFECT TO THE IMPACT ASSESSMENT THAT WOULD OTHERWISE BE COMPLETED PURSUANT TO THIS SUBSECTION.

- Further clarity on what information is both helpful and reasonable for consumers to receive in direct disclosures or while using an interactive artificial intelligence system should occur.

14-47A-07 - Enforcement

- Under (A), clarify that “This Act shall be exclusively enforced by the Attorney General.”
- Language should be added that Attorney General requests for information should be subject to an investigative demand.

- Protections should be added for information provided to the Attorney General by including the following language:

IN RENDERING AND FURNISHING ANY INFORMATION REQUESTED PURSUANT TO A CIVIL INVESTIGATIVE DEMAND ISSUED PURSUANT TO THIS SECTION, A DEVELOPER OR DEPLOYER MAY REDACT OR OMIT ANY TRADE SECRETS OR INFORMATION PROTECTED FROM DISCLOSURE BY STATE OR FEDERAL LAW. IF A DEVELOPER OR DEPLOYER REFUSES TO DISCLOSE, REDACTS, OR OMITS INFORMATION BASED ON THE EXEMPTION FROM DISCLOSURE OF TRADE SECRETS, SUCH DEVELOPER OR DEPLOYER SHALL AFFIRMATIVELY STATE TO THE ATTORNEY GENERAL THAT THE BASIS FOR NONDISCLOSURE, REDACTION, OR OMISSION IS BECAUSE SUCH INFORMATION IS A TRADE SECRET. TO THE EXTENT THAT ANY INFORMATION REQUESTED PURSUANT TO A CIVIL INVESTIGATIVE DEMAND ISSUED PURSUANT TO THIS SECTION IS SUBJECT TO ATTORNEY-CLIENT

PRIVILEGE OR WORK-PRODUCT PROTECTION, DISCLOSURE OF SUCH INFORMATION PURSUANT TO THE CIVIL INVESTIGATIVE DEMAND SHALL NOT CONSTITUTE A WAIVER OF SUCH PRIVILEGE OR PROTECTION. ANY INFORMATION, STATEMENT, OR DOCUMENTATION PROVIDED TO THE ATTORNEY GENERAL PURSUANT TO THIS SECTION SHALL BE EXEMPT FROM DISCLOSURE UNDER THE MARYLAND PUBLIC INFORMATION ACT.

14-47A-08 – Civil Action

- The Civil Action created under this subtitle should be eliminated and replaced with language that “NOTHING IN THIS ACT SHALL BE CONSTRUED AS PROVIDING THE BASIS FOR, OR BE SUBJECT TO, A PRIVATE RIGHT OF ACTION FOR VIOLATIONS OF THIS OR ANY OTHER LAW.”

For more information call:

Andrew G. Vetter
J. Steven Wise
Danna L. Kauffman
Christine K. Krone
410-244-7000

CDT Written Testimony re MD SB 936.pdf

Uploaded by: Ereic Null

Position: FWA



**Testimony of Eric Null, Co-Director, Privacy & Data Program,
Center for Democracy & Technology
Before the Maryland Senate Finance Committee
February 27, 2025**

About CDT

The Center for Democracy & Technology (CDT) is a nonprofit, nonpartisan organization fighting to advance civil rights and civil liberties in the digital age. CDT works on many issues touching on various aspects of artificial intelligence, algorithmic systems, and related technologies. It also has workstreams specifically focused on digital rights in specific fields relevant to automated decisions, including workers' rights and disability rights.

Introduction

We greatly appreciate the effort that Senator Hester and her colleagues have put into crafting SB 936, which would cover automated decision systems (ADSs)¹ in settings as diverse as employment, housing, health care, and criminal justice. We are generally supportive of the transparency provisions in the bill, as they require transparency around key aspects of ADSs. We are also generally supportive of the duty of care placed on developers to take steps to affirmatively prevent algorithmic discrimination.

Unfortunately, as it stands, the bill's loopholes and exemptions would undermine the bill's goals because they essentially allow companies to opt themselves out of complying with the law. Our concern is not hypothetical: [companies have almost entirely ignored](#) New York City's AI-hiring ordinance, which has similar infirmities.

Below, we briefly discuss the problem of companies using hidden algorithms and other ADSs to make key decisions about workers and consumers and how the lack of transparency surrounding such systems poses particular risks to disabled workers and consumers. We then highlight the bill's strong transparency provisions, but discuss how, in its current form, the bill's narrow definitions and overbroad exemptions would make those transparency provisions largely illusory.

We hope that the Committee will take steps to address these issues by fixing the key definitions and closing these loopholes while there is still time to do so. If those changes are made, we would support SB 936.

¹ We use "automated decision system" to refer to the class of technologies that are the subject of SB 936. We do not necessarily oppose the use of the term "high-risk artificial intelligence system" for purposes of this bill, but that term may be confusing since it has also been used to refer to a wide range of other AI applications that also pose risks to large numbers of consumers (such as AI-enabled surveillance systems, deepfakes, etc).

Automated decision systems are frequently hidden from the workers and consumers they effect and carry significant risks, particularly to those from vulnerable and marginalized communities

Artificial intelligence (AI) has seen rapid and genuine progress in recent years. Generative AI systems have allowed for the introduction of consumer-facing chatbots that perform leaps and bounds better than their predecessors from just a few years ago. AI is also showing promise in the areas of scientific and medical research. States can, and should, encourage innovation in those and other areas of AI research that clearly advance the public interest.

But not all applications of AI are beneficial, particularly when it comes to their impacts on vulnerable workers and consumers. Companies increasingly use AI-powered ADSs when determining who to hire, mortgage rates for bank customers, who can access public benefits like SNAP or Medicaid, and how much we all pay for life's necessities like health care and rent. Unfortunately, there is [considerable evidence that many such ADSs are biased](#) (or simply [do not work](#)) and that removing such bias [is quite difficult](#). At the same time, the lack of transparency surrounding companies' ADS practices means that workers, consumers, and regulators only rarely catch glimpses of when, how, and on whom companies use these tools.

We do not have a clear picture of how, nor how many, companies use these technologies because information disclosure about ADS use by companies is sporadic and inconsistent, if there is disclosure of the ADS use at all. That said, considerable anecdotal evidence suggests that the practice is already widespread. Surveys of companies indicate that anywhere from [one-third](#) to [the vast majority](#) already use ADSs in recruitment and hiring alone. But we often don't know *which* companies are using these tools, nor which workers and consumers are being affected by them.

Stories about harmful uses of ADSs have come to light thanks to whistleblowers and investigative journalism. ProPublica has published a trio of reports on how the health care giant Cigna [secretly used](#) an [algorithm](#) to mass-reject policyholders' claims—and then [threatened to fire a physician](#) who pushed back. But consumers and workers should not be forced to rely on whistleblowers and nonprofit news outlets to bring these issues to light, nor to fight harmful ADSs.

The significant information asymmetry surrounding ADSs provides a strong reason for regulation because existing civil rights, labor, and consumer protections cannot be enforced effectively when the role of AI is hidden or obscured. But narrow definitions and overbroad exemptions will render ADS regulations ineffective—[as appears to have happened with New York City's law](#).

The risks associated with hidden ADSs are particularly high for disabled workers and consumers because the systems are often inaccessible or biased against people with disabilities. In the cases where consumers and workers have to interact with the system, as is the case with many automated employment assessments, the systems are often inaccessible and offer people with disabilities few or no options for accommodation or alternative assessment methods.

CDT and allied organizations have found extensive discriminatory impact caused by ADSs. A 2020 CDT report highlighted how algorithmic hiring tools can discriminate against

disabled job candidates, [noting](#) that “as these algorithms have spread in adoption, so, too, has the risk of discrimination written invisibly into their codes.” Last fall, CDT and AAPD released a report, *Screened Out: The Impact of Digitized Hiring Assessments on Disabled Workers*, detailing the findings of a study on disabled workers’ experiences with modern digitized assessments, including automated video game assessments and video interviews. The disabled workers who participated [said that they](#) “felt discriminated against and believed the assessments presented a variety of accessibility barriers.” Notably, SB 936 includes an unqualified exemption for “artificial intelligence-enabled video games,” which would seem to exclude the sorts of gamified assessments that many study participants found inaccessible and discriminatory.

Other CDT publications have highlighted how [electronic surveillance and algorithmic management \(or “bossware”\) systems](#) are used in ways that can violate the rights and threaten the health and safety of disabled workers, how [surveillance technology discriminates](#) against disabled people, and how [tenant screening algorithms](#) can disproportionately exclude disabled people, among other marginalized groups. The Disability Rights Education and Defense Fund (DREDF) published a brief in 2023 describing how algorithms could embed ableist standards of care into health care decision-making, [expressing concern](#) that “algorithmic and AI bias can further stigmatize patients, misdirect resources, and reinforce or ignore barriers to care rather than serving as a pathway to improving treatment and health outcomes.”

These biases and barriers to accessibility cannot be addressed without basic transparency regarding when and how automated decision systems are being used, what those systems measure or assess, and how they measure or assess it. Systems that are unreliable, inaccurate, or biased against individuals with disabilities or people from other marginalized communities likewise will not be detected unless companies conduct impact assessments to identify potential sources of inaccessibility, bias, and invalidity.

We support the substantive transparency requirements in SB 936

The bill’s substantive provisions would grant consumers the right to basic transparency regarding ADSs. The bill’s notice provisions would require covered companies to provide consumers with:

- (a) a description of the personal characteristics or attributes that such system will measure or assess, (b) the method by which the system measures or assesses such attributes or characteristics, (c) how such attributes or characteristics are relevant to the consequential decisions for which the system should be used, (d) any human components of such system, and (e) how any automated components of such system are used to inform such consequential decisions.

Consumers and workers deserve this information as a matter of basic fairness when they are subjected to important decisions that could affect, for instance, their housing, career compensation, health, safety, or economic security. These disclosures are especially crucial for people with disabilities, many of whom need the information to know whether the system might be inaccessible or inaccurate with respect to them and whether the company’s human-review

safeguards provide an adequate opportunity for them to request accommodation or an alternative form of evaluation or decision process.

SB 936's definitions would leave workers and consumers unprotected unless they are amended

The definition of “consumer” excludes workers and could be misused to exclude many consumers

ADSs are being aggressively marketed and implemented in workplaces and labor markets in Maryland and across the country. But the bill's definition of “consumer” explicitly excludes anyone acting “in a commercial or employment context.” This broad and undefined exemption would apparently exclude all workers—employees, independent contractors, and job candidates alike—from the bill's protections.² This means that, despite the fact that the bill contemplates “access to or provision of employment” as a “consequential decision,” those protections would not apply to any Maryland worker. In other words, the bill would provide no protection when employers use inaccessible AI systems or flawed or biased algorithms to decide who to hire and fire and how much workers get paid. Additionally, the term “commercial . . . context” is ambiguous and undefined; for instance, are customers browsing in a retail store acting in a “commercial . . . context” and thus any use of ADSs in that store, such as facial recognition technology that seeks to [identify shoplifters](#), not subject to the bill? The definition of “consumer” thus should be amended to cover all Marylanders.

Recommendation: The definition of “consumer” should simply be: “a natural person who is a resident of this state.”

The bill's definition of “high-risk artificial intelligence system” would make it far too easy for companies to evade the law's transparency requirements

SB 936 defines “high-risk artificial intelligence systems” as systems that are “specifically intended to autonomously make, or be a substantial factor in making” key decisions. This definition is deeply concerning; it would make it far too easy for developers to define themselves out of the law's scope. A company could, for example, completely avoid the bill's obligations—including its obligation to reveal the existence of the system to affected consumers—by crafting technical documentation or marketing materials with a disclaimer saying: “Use only with human supervision” or “Not intended to serve as the principal basis for a decision.” The developer and any deployer that uses the system could then justify to themselves that the ADS is not intended to autonomously make or substantially affect decisions and use that as a justification to ignore the law. It would be almost impossible for a plaintiff to disprove the developer's subjective intent—especially because invoking this definitional loophole would allow companies to keep the system's very existence hidden.

This loophole thus would allow companies to opt themselves out of complying with the law by determining its system is exempt from the law's disclosure obligations. As a result,

2

consumers, outside experts, and enforcers would have no way to learn about the system and challenge that conclusion.

Recommendation: The definition should be amended to eliminate any requirement tied to the developer's or deployer's subjective intent, and should focus on the system's use.

The definitions of “substantial factor” and “principal basis” could allow companies to escape transparency and accountability by having humans rubber-stamp algorithmic “recommendations”

The definitions of “substantial factor” and “principal basis,” as currently written, would allow companies using ADSs to evade the law if there is “human review, oversight, involvement, or intervention” in the decision process or “meaningful consideration by a human” in the decision process. Under this definition, as long as a company assigns a human to review algorithmic “recommendations,” the company could justify to itself that it is exempt, keep the system hidden from affected consumers, and ignore the law's transparency and accountability requirements.

The problem is that companies often claim they have human review for all decisions—but, in reality, those humans can act as rubber stamps or feel pressure to follow algorithmic recommendations, exemplified by the investigative reports on Cigna described above. Thus, as with the “specifically intended” loophole, this provision effectively would provide companies (in this case deployers) an easy avenue to opt out of compliance with the law.

In a brief on disability bias in health care algorithms, DREDF [highlighted](#) how the incorporation of algorithms into decision-making processes can lead humans to abdicate their responsibilities even when there is a genuine desire for humans to bring their own judgment to bear as well:

While DREDF is concerned with how algorithms are created and how developers evaluate the fairness of the formula and data inputs used, the crux of our concern with computer-mediated tools is that the human decision-makers who bear ethical and professional obligations as health care providers and entities have changed their decision-making process. Furthermore, they may choose to do so without any notice of the change. In essence, they may believe they have fully delegated their decision-making authority and should no longer be held accountable for the discriminatory outcomes because computers cannot “intend” discrimination. Once algorithms are involved and assigned a role within decision-making, there is a human tendency to give primary weight to the algorithmic output, decision, or recommendation, even in the face of conflict with human expertise, knowledge, and judgment. Examples of this deference to algorithms can be found in decisions made by pilots who defer to automatic flight control systems, as well as by physicians making treatment decisions in critical care units; the higher the stakes and, some might say, the greater the need for a human grappling with ethics, life values, and implicit bias, the greater the pressure to abdicate responsibility to an “objective” algorithm.

Having a “human in the loop” thus is no panacea. “Substantial factor” requirements and, especially, “human review” exemptions instead introduce loopholes with the potential to dramatically undermine the law.

Recommendation: The “substantial factor” requirement should be eliminated and the definition of “high-risk artificial intelligence system” amended to align with the definition of “high-risk automated decision system” in California Assembly Bill 2885, which was enacted last year and applies to all systems that “assist or replace human discretionary decisions.” That definition would ensure that affected consumers receive notice of any automated decision system used in crucial decisions about them.

SB 936 contains other exemptions and carve-outs that would allow too many companies to avoid compliance, transparency, and accountability

The bill contains several other exemptions that would significantly undermine the bill’s substantive provisions unless they are eliminated.

SB 936 gives companies discretion to ignore disclosure requirements by designating information as “confidential” or “proprietary”

The bill completely exempts information developers consider a “trade secret,” “confidential or proprietary information,” or “a security risk.” These exemptions essentially require total deference to developers in deciding for themselves what information is a “trade secret,” “confidential,” “proprietary,” or a “security risk.”³ Companies frequently over-designate ordinary business information as a trade secret, or confidential or proprietary when it suits them to do so. Infamously, Theranos asserted that information showing its blood-testing technology did not work was a “trade secret”—a fact that only came to light after the company’s fraudulent scheme fell apart. We would not want a similar situation with information about ADSs that cause discrimination being kept secret.

Indeed, the exemption is unnecessary given the modest nature of developers’ disclosure requirements, all of which is information that responsible developers already provide to potential customers quite readily. The bill does not call for any company to disclose its source code, training data, or any other secret sauce that would undermine legitimate intellectual property rights. It simply calls for developers to provide deployers with the information necessary to understand, operate, and manage the system and understand its limitations. A trade secret or confidentiality claim regarding such information would be doubtful at best. That interest should, in any event, yield to the interest in ensuring that deployers have the information they need to comply with their obligations under the law and monitor the performance of systems used in consequential decisions.

Recommendation: These exemptions should be eliminated. If that cannot be done, they should be narrowed—companies should be permitted to redact information only pursuant to trade

³ While “trade secret” is defined in Maryland’s laws [here](#), that definition still gives companies leeway to determine what information has value by being kept secret.

secret law, and when they do, they should be required to alert deployers or other audiences where and why they redacted such information.

The definition of “high-risk artificial intelligence system” should be clarified so that it covers all uses of AI in consequential decisions

The definition of “high-risk artificial intelligence system” contains several additional exemptions that carve entire industries and products out of the bill’s scope. For example, the bill exempts “autonomous vehicles” (AVs). Thus, developers and deployers of AV-related ADSs would be under no obligation to, for instance, protect against known or reasonably foreseeable risks of algorithmic discrimination.

Yet, while future advances in AVs could improve accessibility and lower the cost of travel, there are instances in which decision systems embedded in AVs could pose a significant risk of discrimination. AVs have been known to make decisions on the road that ignored wheelchair users, people who lack limbs, or people with other disabilities that cause them to look or act “atypically.” If AVs are excluded, there would be no protection if an ADS embedded within an AV was trained or learned to pass by humans who have service animals (a common behavior among human drivers) or give priority to traffic and fail to stop at the curb cuts needed by a wheelchair user.

Similarly, the definition of “high-risk artificial intelligence system” exempts “artificial intelligence-enabled video games.” Although the intent may be for this exemption to apply to games used for entertainment, it is problematic as written because AI-enabled video games are a common form of ADS in hiring, and such “games” are often inaccessible to people with disabilities or designed in ways that introduce bias.

Recommendation: All exemptions should either be eliminated or should apply only where ADSs are not used in making a consequential decision.

Exemptions for specific industries should be narrowed

Other exemptions appear to carve out some of the industries that the bill’s definition of “consequential decisions” purports to cover. For example, even though the definition of “consequential decisions” includes financial services, lending, and insurance, § 14-47A-02(2) contains a carve-out exempting insurers subject to the Maryland Insurance Administration (MIA). Insurance companies should have to comply with the bill’s provisions—in particular, where they do not overlap with, for instance, MIA [protections](#) for AI use. Where the requirements are substantially similar, compliance with one should be sufficient for both.

Likewise, § 14-47A-02(1) exempts any system “acquired by” the federal government, and excludes *any* system (except ADSs making employment or housing decisions) that the federal government *ever* acquires—even when those systems are being used by private companies. The implicit justification for this section, that there are additional protections at the federal level for ADSs procured by the federal government, is not always accurate. Further, federal government use of ADSs is already exempt because “person” does not include “government units.”

Recommendation: Exemptions for certain types of ADSs subject to other authorities should apply only where the requirements of this bill and the other authorities are substantially similar. The exemption for ADSs acquired by the federal government should be removed.

Exemption for companies complying with “risk management frameworks” should be removed

The bill also contains an exemption allowing companies to be “presumed to be in conformity” with the bill if they are “in conformity with the latest version of the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology, Standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or internationally recognized risk management framework.” But none of these standards presently comes close to ensuring that consumers receive the information that the bill’s substantive transparency provisions would provide, and it is impossible to predict whether they will be strengthened, weakened, or eliminated as administrations and the composition of standards bodies change. Moreover, the words “another nationally or internationally recognized risk management framework” appear to give companies wide discretion to pick and choose the standards of their liking. This will give rise to inconsistencies and would also make enforcement difficult.

Recommendation: Eliminate the presumption of compliance for companies that conform with non-statutory risk management frameworks.

Companies could escape the right to appeal requirement by invoking a vague “best interest of the consumer” exemption

Individual requirements also contain some loopholes that would allow companies to escape the bill’s obligations. For example, a developer could take away an individual’s right to appeal a decision made by an automated system—an important protection that this bill would rightly give consumers—if the company decides that it is not in “the best interest of the consumer” to let that person appeal the decision. The law does not define what constitutes “the best interest of the consumer;” conceivably, for example, an auto insurance company could say that an appeal of an ADS-driven decision setting a high premium for a consumer is not in the consumer’s best interest because it would delay the consumer’s ability to obtain coverage. Further, the law puzzlingly allows the company in control of the AI system to decide what is in the consumer’s best interest rather than the consumer, who could simply choose not to appeal the decision.

Recommendation: The “best interests of the consumer” exemption should be removed. At the very least, the “best interests” exemption should be significantly clarified and narrowed, much like the right of appeal’s other exemption, which allows appeal denial if there is a delay that poses a risk to the life or safety of a consumer.

Accessibility and accommodation decisions covered by Maryland's human rights laws should be covered consequential decisions

We recommend that the bill's list of consequential decisions be amended to incorporate decisions that grant or deny disabled Marylanders' accessibility and accommodation rights. Maryland has notably provided its residents with some of the country's strongest disability rights protections, with stronger accessibility and accommodation requirements in many cases than federal law provides. But the current list of consequential decisions does not appear to cover, for example, a business's use of ADSs that provide language interpretation and translation services in health care, even though a poorly designed system could easily have the practical effect of denying disabled Marylanders' access to health care.

Recommendation: Add the following to the list of consequential decisions: "(x) a reasonable accommodation or other right granted under the civil rights laws of this state."

Conclusion

While SB 936 aims to address critical risks associated with ADSs, improvements are needed to ensure the bill's provisions provide the intended protection for Marylanders. As it stands, the bill's narrow definitions and ambiguous and overbroad exemptions undermine its otherwise-strong transparency and accountability provisions. To truly safeguard the rights of Marylanders, including and especially those from vulnerable groups, the bill should be amended to close these loopholes and strengthen key definitions. If those changes are made, Maryland will have an opportunity to lead the country with strong legislation empowering its workers and consumers and promoting trustworthy and rights-protecting innovation.

SB 936 CPD Favorable with Amendments.pdf

Uploaded by: Hanna Abrams

Position: FWA

CAROLYN A. QUATTROCKI
Chief Deputy Attorney General

LEONARD J. HOWIE III
Deputy Attorney General

CARRIE J. WILLIAMS
Deputy Attorney General

ZENITA WICKHAM HURLEY
Chief, Equity, Policy, and Engagement



**STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL**

ANTHONY G. BROWN
Attorney General

WILLIAM D. GRUHN
Division Chief

PETER V. BERNIS
General Counsel

CHRISTIAN E. BARRERA
Chief Operating Officer

HANNA ABRAMS
Assistant Attorney General

February 27, 2025

TO: The Honorable Pamela Beidle, Chair
Economic Matters Committee

FROM: Hanna Abrams, Assistant Attorney General
Consumer Protection Division

RE: Senate Bill 936 – Consumer Protection – High-Risk Artificial Intelligence
– Developer and Deployer Requirements
(SUPPORT WITH AMENDMENT)

The Consumer Protection Division of the Office of the Attorney General (the “Division”) supports Senate Bill 936 (“SB 936”), sponsored by Senators Hester, Gile, and Love, with amendments, but urges the Finance Committee to ensure that adequate resources are allocated to ensure proper enforcement. Senate Bill 936 establishes guard rails on the development and use of artificial intelligence to protect Marylanders from discrimination.

The Division supports the General Assembly’s attention to algorithmic harms affecting Marylanders. Algorithm-driven systems are increasingly used to streamline decision-making processes across many significant areas. These systems are designed to execute the steps humans traditionally perform but with far less accountability for discriminatory outcomes. Robust safeguards and restrictions on algorithm-driven decision-making are essential to protecting Marylanders.

Existing law does not address the responsibility of developers or even, in some cases, deployers for the discriminatory harms the artificial intelligence systems they design and deploy cause. The algorithms used are black boxes designed and disseminated by developers and deployers; there is no transparency or accountability. As a result, enforcement of existing anti-discrimination laws to date has not kept up with developments in algorithm-driven decision-making. Senate Bill 936 aims to rectify this gap.

The Division supports SB 936, but believes the following changes are warranted:

Eliminate the rebuttable presumption

The rebuttable presumption contained in SB 936 undermines its purpose and interferes with enforcement. Senate Bill 936 includes a “rebuttable presumption” that developers and deployers

“used reasonable care as required under this subsection if the developer/deployer complied with the provisions of this section.” This significantly delays any resolution by requiring that the Division demonstrate lack of reasonable care twice—first to overcome the rebuttable presumption, and then to demonstrate the violation. The evidence for both would likely be the same, but the requirement to overcome a rebuttable presumption thwarts consumer protection and delays consumer relief. The rebuttable presumption undermines the intent of consumer protection laws, which are meant to safeguard consumers. Md. Code, Com. Law § 13-102.

The bill also includes a non-lapsing cure period that weakens its protections. Cure periods are intended to avoid penalizing companies while innovative legislation is rolled out. However, cure periods nevertheless require the Division to expend resources to investigate a violation but, unlike a case filed or settled by the Division, the company’s conduct is not under any specific future constraints and the Division does not receive reimbursement for the costs expended in investigating the matter. If a cure period is included in SB 936, it should mirror the cure period included in the Maryland Online Data Privacy Act. Com. Law § 14-4614. The cure period should be: (1) at the Division’s discretion; and (2) should sunset after one year. *Id.*

Loopholes must be closed

The loopholes contained in SB 936, if interpreted broadly, could undermine the very protections that the bill intends to provide. The bill exempts AI technology that performs “narrow procedural task[s]” from its definition of high-risk AI. This term is undefined, and companies may argue that all manner of high-stakes decisions – screening out resumes, scoring college applicants – are “narrow procedural tasks.” The bill’s trade secret and confidential information protections are overbroad. Companies should not be able to unilaterally withhold crucial information or hide evidence of discrimination by claiming that such information is a trade secret or confidential information.

Enforcement resources must be allocated

Senate Bill 936 requires extensive manpower and technological resources in order to properly investigate potential violations. Moreover, as discussed above, the inclusion of a non-lapsing right to cure is contrary to consumer protection and undermines the ability of the Division to recover the costs of an investigation. This, along with the inclusion of the rebuttable presumption, will increase the resources necessary if SB 936 is to be enforced.

Ensure that existing antidiscrimination laws are not weakened

The bill should clarify that compliance with SB 936 cannot be used as a shield in cases alleging violations of traditional anti-discrimination laws by either expressly stating that there are no unintended consequences or by linking violations of SB 936 to violations of the Consumer Protection Act.

Line Amendments

- p.4, line 15: Since artificial intelligence systems are not generally “offered, sold, leased, [or] given,” the following language should be added at the end of the line: “or otherwise impacts a consumer in the state”

- p. 5, lines 13-14: It is not clear what the exclusion “improve the result of a previously completed human activity” means. This should be removed from the exclusions or clarified.
- p. 6, line 18: An “intentional and substantial modification” should include any previously unassessed risk of algorithmic discrimination. The word “material” should be replaced with “previously unassessed.”
- p. 9, lines 14-18 and p. 13, lines 26-30: These lines should be deleted. As explained above, a rebuttable presumption delays consumer relief and duplicates the work necessary to prosecute alleged algorithmic discrimination.
- p.12, lines 1-14 and p. 14 line 32 - p.15 line 11: NIST’s Artificial Intelligence Risk Management Framework and ISO/IEC 42001 provide guidelines and best practices for managing risk and are intended as flexible frameworks, rather than a checklist. Similar to the rebuttable presumption, it would complicate investigations to establish a presumptive safe harbor.
- p. 12, lines 17-23: It should be clarified that “trade secret” cannot be used as a shield to hide information from the Attorney General during an investigation. In addition, the trade secrete exemption should be narrower.
- p. 21, lines 13-19: Violations of SB 936 should be linked to the Consumer Protection Act. Lines 13-19 should be deleted and replaced with the following language: “A violation of this subtitle: (1) is an unfair, abusive, or deceptive trade practice; and (2) except for the provisions of § 13-411 of the Commercial Law Article, is subject to the enforcement and penalty provisions contained in Title 13 of the Commercial Law Article.”
- p. 22, line 4: It should be clarified that the Attorney General may require a developer or deployer to disclose any information that is necessary to assess compliance with the subtitle.
- p. 22, line 10: replace “shall” with “may” and the availability of the cure period should lapse October 1, 2027.

Accordingly, we urge the Finance Committee to issue a favorable report on SB 936 with the amendments discussed.

cc: Members, Finance Committee
The Honorable Katie Fry Hester
The Honorable Dawn Gile
The Honorable Sara Love

SB0936_MDVCC_Kilbane_FWA.pdf

Uploaded by: Matthew Kilbane

Position: FWA

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

Matthew H. Kilbane
Legislative Director
Maryland Veterans Chamber of Commerce
6707 Cherryfield Road
Ft. Washington, MD 20744
matthew.h.kilbane@outlook.com
+1-240-946-0224

16JAN2025

The Honorable Pamela Beidle
Finance Committee
3 East Miller Senate Office Building
Annapolis, MD 21401

Dear Chairperson Beidle and Members of the Committee,

We support the proposed legislation that, “Requiring a certain developer of, and a certain deployer who uses, a certain high-risk artificial intelligence system to use reasonable care to protect consumers from known and reasonably foreseeable risks of certain algorithmic discrimination in a certain high-risk artificial intelligence system; regulating the use of high-risk artificial intelligence systems by establishing certain requirements for disclosures, impact assessments, and other consumer protection provisions.”. As the Legislative Director of the Maryland Veterans Chamber of Commerce, I advocate for policies that protect our citizens and promote the ethical use of technology.

The inclusion of consumer protections in the legal and regulatory framework is a crucial step in ensuring that our laws keep pace with technological advancements. AI technology has the potential to create realistic images, text, and video that can be misused, making it essential to update our legal definitions to encompass these new forms of media and prevent exploitation.

Moreover, the lack of comprehensive AI legislation in the State of Maryland is detrimental to both our citizens and businesses. The absence of clear guidelines and regulations creates uncertainty and poses risks to privacy, security, and ethical standards. Maryland should create a strong regulatory agency (Maryland AI Regulatory Agency, MARA) to govern responsible AI development and operations by following principles outlined in other regions (e.g. EU AI Act, Canadian AI & Data Act, etc.).

An active and engaged regulatory body is necessary to enforce transparency, accountability, and fairness in the development and deployment of AI technologies. Additionally, the agility present within the body of subject matter experts positions MARA to mitigate economic (job loss, displacement, etc.), social (Does an entity born of artificial general intelligence (AGI) have rights?), and ethical (If an AGI instance is deleted, is the person who pushed the button guilty of murder?) issues that are on the horizon. Failure to act may result in the unchecked proliferation of AI applications that could harm individuals and erode public trust in technology, government, and our society.

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

We urge the committee to favorably consider this legislation and to read the appended draft of the Maryland Artificial Intelligence Regulation Act (MAIRA). This act provides a comprehensive approach to governing AI technologies, ensuring that Maryland remains at the forefront of ethical and responsible AI innovation.

Thank you for your attention. We look forward to your response.

Sincerely,

Matthew Kilbane



Legislative Director,
Maryland Veterans Chamber of Commerce

In the absence of specific legislation regulating artificial intelligence (AI) in the United States, the American public faces significant risks and challenges. Without clear legal frameworks, AI technologies can be deployed without adequate oversight, leading to potential abuses and unintended consequences. The lack of regulation allows for the development and use of high-risk AI systems that could infringe on individuals' privacy, perpetuate biases, and make critical decisions without transparency or accountability. This vacuum leaves citizens vulnerable to the whims of private entities and foreign actors who may not prioritize ethical considerations or the public good.

Furthermore, the absence of US-specific AI legislation hampers the country's ability to compete globally in the rapidly evolving AI landscape. Other nations are forging ahead with comprehensive regulatory frameworks that ensure safe, fair, and innovative AI development. Without similar measures, the United States risks falling behind in both technological advancement and ethical leadership. This legislative gap not only compromises public trust in AI but also jeopardizes the nation's position as a leader in technological innovation and governance.

The proposal below is my attempt to bridge that gap for the State of Maryland and I firmly believe that similar legislation is needed at the Federal level to ensure that we, as a Nation, are all to continue establishing justice, ensuring domestic tranquility, providing for the common defense, and promote the general welfare of our society for generations to come.

DRAFT for legislation to govern Artificial Intelligence in the State of Maryland

Maryland Artificial Intelligence Regulation Act (MAIRA)

Section 1: Purpose and Scope

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

1.1 The purpose of this Act is to ensure the ethical and responsible development, deployment, and use of Artificial Intelligence (AI) systems within the State of Maryland.

1.2 This Act applies to all AI systems developed, deployed, or used within the State of Maryland by public and private entities.

Section 2: Definitions

2.1 **Artificial Intelligence (AI) System:** A machine-based system that can, for a given set of human defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing real or virtual environments.

2.2 **High-Risk AI System:** AI systems that pose significant risks to the health, safety, and fundamental rights of individuals.

2.3 **Fairness and Non-Discrimination:** Ensuring that AI systems are designed and implemented in a manner that prevents discrimination against individuals based on race, gender, age, disability, or any other protected characteristic.

2.4 **Transparency:** Providing clear and accessible information about the AI system's capabilities, limitations, and the data it uses, as well as disclosing the purpose and intended use of AI systems to users and affected individuals.

2.5 **Accountability:** The responsibility of entities deploying AI systems to ensure their proper functioning and compliance with this Act, including appointing a designated officer or team to oversee the ethical deployment and operation of AI systems.

2.6 **Privacy and Data Protection:** Compliance with existing data protection laws, ensuring the anonymization or pseudonymization of personal data, and implementing robust data security measures to protect individual privacy.

2.7 **Reliability and Safety:** Rigorous testing of AI systems to ensure they operate reliably and safely under various conditions, establishing safety protocols, and continuous monitoring and maintenance of AI systems.

2.8 **Inclusiveness:** Designing AI systems to be inclusive and accessible to all individuals, including those with disabilities, and involving diverse groups in the development and testing of AI systems.

2.9 **Human Oversight:** Designing AI systems to complement human decision-making, allowing for human intervention in the operation of AI systems, especially in high-risk scenarios, and providing training programs to ensure individuals understand the capabilities and limitations of AI systems.

2.10 **Impact Assessments:** Evaluations conducted to identify and mitigate potential risks associated with high-risk AI systems.

2.11 **Maryland AI Regulatory Authority (MARA):** The body established to oversee the implementation and enforcement of this Act, responsible for issuing guidelines, conducting audits, and imposing penalties for non-compliance.

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

2.12 Public Consultation: The process of involving the community in the development and deployment of high-risk AI systems to ensure transparency and community involvement.

2.13 Penalties: Fines, suspension of operations, or other penalties imposed on entities found in violation of this Act.

Section 3: General Principles

3.1 Fairness and Non-Discrimination:

- AI systems must be designed and implemented in a manner that ensures fairness and prevents discrimination against individuals based on race, gender, age, disability, or any other protected characteristic.
- Developers and deployers of AI systems must conduct regular audits to identify and mitigate biases in AI algorithms and data sets.
- Mechanisms must be in place to allow individuals to report instances of discrimination or unfair treatment resulting from AI systems.

3.2 Transparency:

- Clear and accessible information must be provided about the AI system's capabilities, limitations, and the data it uses.
- Entities must disclose the purpose and intended use of AI systems to users and affected individuals.
- AI systems must be designed to provide explanations for their decisions and actions, enabling users to understand how outcomes are generated.

3.3 Accountability:

- Entities deploying AI systems are responsible for ensuring their proper functioning and compliance with this Act.
- A designated officer or team must be appointed to oversee the ethical deployment and operation of AI systems.
- Entities must maintain detailed records of AI system development, deployment, and performance to facilitate audits and investigations.

3.4 Privacy and Data Protection:

- AI systems must comply with existing data protection laws, including the Maryland Data Privacy Act and other relevant regulations.
- Personal data used by AI systems must be anonymized or pseudonymized to protect individual privacy.

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

- Entities must implement robust data security measures to prevent unauthorized access, use, or disclosure of personal data.
- Users must be informed about the data collection practices of AI systems and provided with options to control their data.

3.5 Reliability and Safety:

- AI systems must be rigorously tested to ensure they operate reliably and safely under various conditions.

Safety protocols must be established to address potential failures or malfunctions of AI systems.

- Continuous monitoring and maintenance of AI systems are required to ensure they remain safe and effective over time.

3.6 Inclusiveness:

- AI systems must be designed to be inclusive and accessible to all individuals, including those with disabilities.
- Efforts must be made to involve diverse groups in the development and testing of AI systems to ensure they meet the needs of all users.

3.7 Human Oversight:

- AI systems must be designed to complement human decision-making, not replace it.
- Mechanisms must be in place to allow human intervention in the operation of AI systems, especially in high-risk scenarios.
- Training programs must be provided to ensure that individuals interacting with AI systems understand their capabilities and limitations.

Section 4: Requirements for High-Risk AI Systems

4.1 Rigorous Testing and Validation:

- High-risk AI systems must undergo comprehensive testing and validation to ensure their safety, reliability, and compliance with ethical standards.
- Testing must include simulations and real-world scenarios to evaluate the system's performance under various conditions.

4.2 Impact Assessments:

- Entities must conduct thorough impact assessments to identify and mitigate potential risks associated with high-risk AI systems.
- Impact assessments must consider the potential effects on health, safety, privacy, and fundamental rights of individuals.

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

4.3 Continuous Monitoring and Evaluation:

- High-risk AI systems must be subject to continuous monitoring and evaluation to ensure ongoing compliance with safety and ethical standards.
- Entities must establish mechanisms for real-time monitoring and periodic reviews of AI system performance.

4.4 Risk Mitigation Strategies:

Entities must develop and implement risk mitigation strategies to address identified risks and vulnerabilities in high-risk AI systems.

- Risk mitigation strategies must include contingency plans for potential failures or malfunctions.

4.5 Documentation and Reporting:

- Entities must maintain detailed documentation of the development, deployment, and operation of high-risk AI systems.
- Regular reports on the performance, risks, and compliance of high-risk AI systems must be submitted to the Maryland AI Regulatory Authority (MARA).

Section 5: Governance and Oversight

5.1 Establishment of MARA:

- The Maryland AI Regulatory Authority (MARA) is established to oversee the implementation and enforcement of this Act.
- MARA will be composed of experts in AI, ethics, law, and public policy.

5.2 Responsibilities of MARA:

- MARA is responsible for issuing guidelines, conducting audits, and imposing penalties for non-compliance.
- MARA will develop and maintain a registry of high-risk AI systems deployed within the state.
- MARA will provide advisory services to entities developing or deploying AI systems to ensure compliance with this Act.

5.3 Audit and Compliance:

- MARA will conduct regular audits of AI systems to ensure compliance with this Act.
- Entities must cooperate with MARA during audits and provide access to necessary documentation and data.

5.4 Public Reporting:

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

- MARA will publish annual reports on the state of AI deployment in Maryland, including compliance statistics and identified risks.

Section 5.1: Governance and Regulatory Responsibility for Artificial General Intelligence

The governance and regulatory responsibility for Artificial General Intelligence (AGI) is crucial to ensure the ethical and safe development, deployment, and use of AGI systems. The following principles and guidelines are proposed to address the unique challenges posed by AGI:

- 5.1.1 Establishment of a Dedicated Regulatory Body:** A specialized regulatory body should be established to oversee AGI development and deployment. This body will be responsible for creating and enforcing regulations, conducting audits, and ensuring compliance with ethical standards.
- 5.1.2 Ethical Frameworks and Guidelines:** The regulatory body should develop comprehensive ethical frameworks and guidelines for AGI. These frameworks should address issues such as fairness, transparency, accountability, privacy, and safety.
- 5.1.3 Risk Assessment and Mitigation:** Entities developing AGI systems must conduct thorough risk assessments to identify potential risks and vulnerabilities. Risk mitigation strategies should be implemented to address these risks and ensure the safety and reliability of AGI systems.
- 5.1.4 Public Consultation and Stakeholder Engagement:** Public consultation and stakeholder engagement are essential to ensure transparency and community involvement in AGI governance. Entities must engage with a diverse range of stakeholders, including community groups, industry experts, and advocacy organizations.
- 5.1.5 Continuous Monitoring and Evaluation:** AGI systems must be subject to continuous monitoring and evaluation to ensure ongoing compliance with safety and ethical standards. Regular audits and performance reviews should be conducted to identify and address any issues.
- 5.1.6 International Collaboration:** Collaboration with international regulatory bodies and organizations is necessary to develop harmonized standards and guidelines for AGI. This will ensure that AGI development and deployment are aligned with global best practices.
- 5.1.7 Education and Training:** Comprehensive education and training programs should be provided to individuals involved in AGI development and deployment. These programs should cover ethical considerations, regulatory requirements, and technical aspects of AGI.

Section 6: Public Participation and Consultation

6.1 Public Consultation Process:

- Public consultation is required for the development and deployment of high-risk AI systems to ensure community involvement and transparency.

Letter of Support for SB0936 Consumer Protection – High-Risk Artificial Intelligence – Developer and Deployer Requirements

- Entities must provide clear and accessible information about proposed AI systems and their potential impacts.

6.2 Stakeholder Engagement:

- Entities must engage with a diverse range of stakeholders, including community groups, industry experts, and advocacy organizations, during the consultation process.
- Feedback from stakeholders must be documented and considered in the development and deployment of AI systems.

6.3 Transparency in Consultation:

- The results of public consultations must be made publicly available, including how feedback was addressed and incorporated into the AI system's design and deployment.

Section 7: Penalties and Enforcement

7.1 Penalties for Non-Compliance:

- Entities found in violation of this Act may be subject to fines, suspension of operations, or other penalties as deemed appropriate by MARA.
- Penalties will be proportionate to the severity of the violation and the potential harm caused.

7.2 Enforcement Mechanisms:

- MARA will have the authority to issue enforcement notices, requiring entities to take corrective actions to address non-compliance.
- In cases of severe or repeated violations, MARA may revoke the authorization to deploy high-risk AI systems.

7.3 Appeals Process:

- Entities subject to penalties or enforcement actions may appeal MARA's decisions through an established appeals process.
- The appeals process will be transparent and provide entities with an opportunity to present their case.

Section 8: Effective Date

8.1 Implementation Timeline:

- This Act shall take effect on [Effective Date].
- Entities must comply with the requirements by [Effective Date].

– Nothing Follows –

SB 936 High-Risk Artificial Intelligence APCIA SWA

Uploaded by: Nancy Egan

Position: FWA

Testimony of

American Property Casualty Insurance Association (APCIA)

Senate Finance Committee

Senate Bill 936 - Consumer Protection - High-Risk Artificial Intelligence - Developer and Deployer Requirements

February 27, 2025

Support with Amendments

The American Property Casualty Insurance Association (APCIA) is the primary national trade organization representing nearly 71.4 percent of the Maryland property casualty insurance market. APCIA appreciates the opportunity to provide written testimony in regards to Senate Bill 936.

Senate Bill 936 addresses the regulation of Artificial Intelligence by defining it as well as regulating those deploying and developing this technology and its impact in Maryland. APCIA is asking for an amendment to the bill to remove certain language. The insurance industry, including property and casualty insurers, is committed to ensuring that algorithms are free from unfair discrimination. We are seeking to have the insurance industry removed from the scope of the legislation for the following reasons:

1. The business of insurance is regulated by the states, overseen by Insurance commissioners in each of the 50 states and the District of Columbia. The National Association of Insurance Commissioners (NAIC) is a non-governmental body comprised of state insurance commissioners and staff.
2. The NAIC establishes recommended minimum standards for capital standards and other prudential requirements that are largely uniform when adopted across the states. Including insurance within the scope of the draft legislation would subject insurance companies, operating in the Maryland, to entirely separate and possibly conflicting requirements on the use of algorithms and predictive models. These additional requirements would impact affordability and availability of products in Maryland negatively impacting Maryland residents.
3. Maryland insurance regulation law includes robust oversight- and regulations under which insurers currently operate. These include privacy protections, safeguarding health information and restrictions on unfair discrimination. The existing regulatory system already applies to the use of AI as well as to more traditional means of implementing the business of insurance. The Maryland insurance regulators are well-equipped to address any illegal use of algorithms, machine learning and artificial intelligence by insurers with a full range of enforcement tools, including fines, license revocation and investigations.
4. The NAIC has established a committee to address data issues with the highest priority on the use of AI, algorithms, machine-learning and accelerated underwriting. The goal of which is to create a uniform approach to regulating these activities so that consumers are protected equally and fairly across all jurisdictions rather than having a patchwork of protections from state to state.
5. Most importantly, the nation's insurance regulators through the NAIC have drafted the AI Model Bulletin, which Maryland has adopted. That bulletin reiterates applicable law and includes the key components of responsible AI including notice, governance, transparency and anti-discrimination provisions but does so

in a way to support the competition and solvency of Maryland's insurance sector. There is simply no need for more or different regulation by another government agency, as the issue has been fully addressed in the insurance context.

6. With the adoption of the AI Model Bulletin in Maryland regulation, the insurance commissioner is already has the power to examine insurers' use of algorithms and predictive models. The inclusion of insurance within the scope of this legislation could seriously impair or impede those activities.
7. Protecting insurance consumers includes maintaining a robust and competitive insurance market. The Insurance Commissioner and staff are uniquely qualified to maintain the appropriate balance between the imposition of regulatory burdens and consumer protection to create the conditions for a healthy insurance market within the Commonwealth.

It appears that on first glance insurers are removed from the bill on page 8 lines 22-36:

THIS SUBTITLE DOES NOT APPLY TO: ...(2) AN INSURER, OR A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM DEVELOPED OR DEPLOYED BY AN INSURER FOR USE IN THE BUSINESS OF INSURANCE, IF THE INSURER IS REGULATED AND SUPERVISED BY THE INSURANCE ADMINISTRATION ~~AND SUBJECT TO THE PROVISIONS UNDER TITLE 13 OF THIS ARTICLE;~~

However, APCIA is concerned about the phrase requiring insurers to be "subject to the provisions under title 13 of this article" to qualify for the exemption. Under Article 13 of Maryland Commercial Law., insurance companies are exempt from article 13 of the Commercial Law under MD COML § 13-104. That means insurers won't actually be able to qualify for the exemption in this AI bill because they are not "subject to the provisions under title 13...".

We are asking that the above language deleted at line 25-26 so we can actually qualify for this exemption. We believe this may have been an oversight in drafting.

APCIA respectfully requests this amendment on Senate Bill 936.

Nancy J. Egan,

State Government Relations Counsel, DC, DE, MD, VA, WV

Nancy.egan@APCIA.org Cell: 443-841-4174

Russell Harris Testimony re SB 936.pdf

Uploaded by: Russell Harris

Position: FWA

Concerns About MD SB 936 regarding Artificial Intelligence, Consumer Protection, and Developer and Deployer Requirements

Testimony of Russell Harris Bowie, Maryland

Senator Hester and Committee Members:

Thank you for the opportunity to testify today about SB 936, regarding High-Risk Artificial Intelligence and Consumer Protection.

I am Russell Harris. I'm testifying today because it is so important that legislators appreciate the treasures you have here in Maryland, including a powerful cadre of AI-powered startups that could change the world and drive Maryland's economy to greater heights than ever before.

For eighteen months I was an Investment at Techstars, the nationally acclaimed startup incubator that has quietly been building a HealthTech program at Johns Hopkins Medical School. My primary role was to review more than 3,000 applications from AI-powered startups that hope to spend several months in Baltimore working with Techstars and Johns Hopkins.

For several decades, Maryland has been an extraordinary place to start and build software companies. Many people know of Maryland's life sciences leadership, but ed-tech and health-tech startups also thrive here. Amidst this exciting opportunity that's only beginning, I urge you to consider AI regulation with one eye on protecting consumers and another focused like a laser on maintaining Maryland's startup and software leadership. It's easy to get big-footed by Silicon Valley and New York's Silicon Alley, so it's important that Maryland proudly and loudly focuses on the prize that is AI opportunity.

As a Black Man, I care deeply about bias and discrimination. I've been discriminated against, so I'm pleased that Maryland has comprehensive anti-discrimination laws and a history of strong enforcement.

Let me be clear: No software - AI or not - should make or substantially influence unlawfully discriminatory consequential decisions. But this bill is all about process, paperwork, and more process, all focused on ensuring that startups think about, evaluate, mitigate, monitor, document internally and externally, and communicate risks of discrimination and countermeasures they have taken. These are righteous goals, but the bill's evaluation and documentation requirements are four pages long. The risk assessment, notice, disclosure, and human appeal obligations are extraordinary - requiring AI-powered consequential decisions to have disclosures and appeals processes that have never previously been required for software-powered or -influenced decisions.

AI is a force multiplier. Used for good, AI helps companies with three people compete against companies with 300 or 3,000 people. AI means capital-starved minority-owned businesses can succeed in ways never before possible. But if compliance overwhelms a startup's small team, and requires a fourth, fifth, or sixth employee to oversee evaluations and documentation instead of building products that scale - that would be the end. Investors carefully scrutinize how funds are used, and if the compliance burden is excessive they will quickly shift to investing in competing states instead of Maryland.

There are so many good reasons for AI system developers and deployers to use anti-bias quality control and assurance practices. First, because they want to build great products. Second, the consequential decisions implicated by the bill all involve regulated industries where discrimination is a known risk. Procurement teams and lawyers in healthcare, education, insurance, and financial services are trained to ensure their people and services are not unlawfully biased, so AI product developers know they will be scrutinized by prospective customers and have to answer these hard questions in the sales process.

But if this legislation becomes law, founders and investors will have another, very unpleasant reason to think about bias - and to document that we're thinking about it. Because if we don't evaluate or document adequately, we could be investigated by the Attorney General, fined, publicly shamed, and perhaps bankrupted by private lawsuits. Those risks - and that our view of what is foreseeable or how to communicate risks may differ from the Attorney General's view - change the investment and startup analysis substantially and negatively because then we'll have to hire expensive lawyers or consultants to confirm the adequacy of our work.

It is also notable that this bill includes a private right of action that is not limited to ensuring the adequacy of a company's processes. Notwithstanding Maryland's very strong technology-neutral discrimination law that already applies, the bill creates a new cause of action for "discrimination by AI," which seems wholly unnecessary and reinforces my concern that this bill will drive investors away.

In addition to sharing concerns, I'm happy to make some concrete suggestions that will improve the bill.

1. Remove the private right of action, which is a frightening deterrent to Maryland companies building and adopting AI tools. MD residents who are discriminated against already have robust avenues for redress, and it's unclear why discrimination involving AI should have different rules.
2. Remove the requirement for human appeal if someone is denied a service. Today, though software is a significant component of decisionmaking, human appeals are not required when employment and loan applications are unsuccessful, when kids don't get into college or Gifted & Talented programs, or when someone is rejected by a clinical trial or experimental treatment program. In circumstances where the legislature or regulators have carefully considered specific rights of appeal, such as with health

insurance and car insurance, the law provides for them. But broad rights of human appeal simply because software is involved is not justified at this time.

3. With regard to documentation, disclosure, and risk assessments:
 - Eliminate the requirement to disclose how an AI system operates, including the disclosures of how personal characteristics are assessed and the system logic. These are far beyond what a consumer would be informed about if a decision is made without AI, and publicizing this information could make it easy for people to game the system.
 - Additionally, the data disclosure and correction obligations may already exist in Maryland's privacy law. Having two laws and potentially different regulations and enforcement positions can create unnecessary uncertainty and conflicts.
4. Improve the right to cure by:
 - Make it applicable in all cases instead of providing the Attorney General with discretion. This is a process law, and non-compliance does not indicate that a product or service is making unlawfully discriminatory decisions.
 - Change the cure period from 45 days to 90 days so a firm has adequate time to review the notice of non-compliance, engage legal counsel, and complete a comprehensive review, risk assessment, and documentation process that the legislation anticipates.

Thank you for considering my views.

MD SB 936 (Hester) - oppose.pdf

Uploaded by: Aden Hizkias

Position: UNF



February 27, 2025

The Honorable Pamela Beidle
Chair, Senate Committee on Finance
Room 3 East Wing, Miller Senate Office Building
11 Bladen Street
Annapolis, MD 21401

Re: Please oppose SB 936 and protect AI innovation in Maryland

Dear Chair Beidle and members of the committee:

On behalf of the Chamber of Progress, a tech industry association supporting public policies to build a more inclusive society in which all people benefit from technological advances, **I respectfully urge you to oppose SB 936**, which would stunt Marylander's budding innovative AI tech sector without meaningfully advancing civil rights.

AI has tremendous potential for improving education, enabling creative expression, and creating new business opportunities. So, it is critically important that public policy promotes the broad and equitable distribution of these innovations.

Policymakers are justly concerned about civil rights abuses, particularly discrimination in housing, employment, or lending. Historically marginalized communities have faced repeated discrimination in these areas and many more, and as such, we applaud the sponsors for their attention to these critical matters of social justice.

However, pinpointing the source and catalyst of discriminatory outcomes of an AI system is not always possible, nor is consistently determining who or what is responsible for the act of discrimination.¹ The roots of bias may be in the data used to train a model—which could be laden with human-created biases—or the human who rubber stamps the outcome of an automated decision tool - or from any number of other sources. Regardless of origins, there must be avenues to address circumstances of discrimination that are consistent, whether the abuse is online or offline.

¹ John Villasenor, *Artificial Intelligence and Bias: Four Key Challenges*, BROOKINGS (Jan. 3, 2019), <https://www.brookings.edu/articles/artificial-intelligence-and-bias-four-key-challenges/> ("An additional challenge is that biases can be created within AI systems and then become amplified as the algorithms evolve.").

SB 936's notice requirement jeopardizes sensitive business intelligence and trade practices

The bill's requirement in Section 14-47A-04(D)(1)-(2) that online platforms notify consumers every time a high-risk AI automated decision tool is used to make a consequential decision presents a complex challenge for deployers and developers. While addressing harmful algorithmic discrimination is laudable, such notices could divulge sensitive information about algorithms and data processing methods, potentially compromising user privacy.

For example, SB 936 requires a covered platform to notify a user every time an AI decides whether they qualify for a loan or insurance based on personal data, it might reveal details about the data used, such as credit history, social media activity, or browsing habits. These notifications might allow bad actors to reverse-engineer the AI's decision-making process, making it easier to manipulate or exploit the system. While transparency is important, this approach could unintentionally threaten user privacy and security.

SB 936's impact assessment requirement will burden startups and harm competition

Under Section 14-47A-04(C), the impact assessment further threatens to expose business strategy and stifle competition by mandating that businesses disclose the details of their automated decision tools to the government. Any such disclosure of sensitive business practices must serve a compelling government interest and be narrowly tailored. SB 936 comes up short on both.

While redacting trade secrets may offer some protection, the bill's extensive requirements risk handing proprietary strategies to competitors, giving them valuable insights that would undermine competition and ultimately harm consumers.

Furthermore, SB 936's stifling of AI startups and innovation is in direct contrast to the Moore-Miller Administration's 2025 Economic Growth Agenda that seeks to bring tech industries and jobs, including AI, to Maryland to "spur business growth and build an economy that works for everyone."²

SB 936 will cost Maryland's AI Market

The US AI market is estimated to be worth \$66.2 billion as of 2025. According to Superside, Maryland accounts for 2.50% of AI searches in the country. If we apply this percentage to the US AI market, it comes to \$1.66 billion. The costs for following rules and regulations, like those in SB 936, are estimated to be 17.22% of that amount, which

² See

<https://governor.maryland.gov/news/press/pages/governor-moore-announces-economic-growth-agenda-for-the-2025-legislative-session.aspx>

means compliance costs in Maryland will be around \$285 million. Every time the AI models are updated, another \$285 million in compliance costs will be added. These recurring compliance costs are significant and could add up quickly, making operating AI-related businesses in Maryland more expensive. This could result in higher operational expenses for companies and potentially affect profitability and growth in the sector. (See Appendix for more details.)

Innovators agree that bias is bad

Unfairly biased outcomes are problematic for developers, deployers, and end-users alike. Tech companies are increasingly investing in internal teams for proactive bias detection and mitigation in their products. For example, Google has implemented its 'Responsible AI Practices.'³ The initiative encompasses detailed guidelines for evaluating training metrics in machine learning models, including a thorough examination of the training data itself. Google's practices also emphasize a human-centric approach to AI development. Prioritizing safe and inclusive user experiences remains a top commitment for the tech industry.

SB 936 lacks incentive for “good” developer behavior

We commend the sponsors of SB 936 for integrating a notice-and-cure period under Section 14-47A-07(C)(2), allowing for corrective actions before imposing penalties. However, concerns arise with the bill granting the Attorney General wide-ranging powers to mandate remedies that could adversely affect essential business operations, potentially compromising service functionality, quality, and integrity. Additionally, it's crucial to recognize that smaller firms and startups with limited resources may require more time than established tech giants to detect and rectify discriminatory practices.

Strengthening Maryland's consumer and civil rights laws is a better approach

SB 936 is designed to address potential discrimination from artificial intelligence systems, including automated decision-making, in employment, housing, and other areas. To reiterate, we agree that discrimination is wrong, but focusing exclusively on AI systems ignores offline discrimination; Chamber of Progress opposes bias, whether by human or algorithmic decision-making. A better approach is to strengthen existing civil rights and Maryland fair housing laws to ensure that the most vulnerable members of society are protected online and offline.

For these reasons, **we respectfully urge you to oppose SB 936.**

Thank you,

³ Google, *Responsible AI Practices*, AI.GOOGLE. <https://ai.google/responsibility/responsible-ai-practices/>

A handwritten signature in black ink, appearing to read "Brianna January". The signature is fluid and cursive, with the first name "Brianna" written in a larger, more prominent script than the last name "January".

Brianna January

Director of State & Local Government Relations, Northeast US



Economic Impact of SB 936: A Chamber of Progress Analysis

AI Discrimination Bill May Cost Maryland Developers and Deployers Millions

Maryland's Senate Bill 936 ([SB 936](#)) seeks to regulate high-risk AI systems to prevent algorithmic discrimination, defined as AI-driven decisions causing unlawful differential treatment or disparate impact. The bill imposes compliance requirements on AI developers and deployers, including risk management, transparency, and consumer protections to ensure fairness. Given the significant compliance costs associated with reporting and risk management, Maryland should weigh these financial impacts when considering the bill's passage.

Estimating the Cost of Compliance in Maryland

- **Compliance costs equal to 17.22% of the total cost to build the AI tool**
 - A [report](#) prepared for the European Commission, written by CEPS, ICF, and Wavestone, estimates compliance costs for complying with the EU's AI Act.
 - AI Act imposes requirements on developers and deployers of algorithmic technology, including high-risk AI, in order to avoid discrimination.
 - Their approach utilizes the Standard Cost Model, a model used worldwide and by nearly all EU member states, to estimate the compliance costs as a percentage of total model development costs for the AI Act.
 - Their analysis used interviews with industry stakeholders to confirm assumptions about time and cost estimates.
 - The report estimates compliance costs for the following categories: training data, document and record keeping, provision of information, human oversight, and robustness and accuracy.
 - Their findings suggest compliance costs to be equal to 17.22% of the total cost to build the AI model.
- **Cost Estimate for Maryland - \$285 million**
- The U.S. AI market is [estimated](#) to be worth \$66.2 billion as of 2025.
- As a proxy for AI use within the state, I use the percentage of US searches for AI within Maryland as reported by Superside in [this article](#).
- According to Superside, Maryland was responsible for 2.50% of AI searches in the US.
- Applying 2.50% to the US AI market yields a total dollar amount of \$1.66 billion.
- Compliance costs are estimated to be 17.22% of the total dollar amount of \$1.66 billion, thus compliance costs in Maryland are estimated to be \$285 million. For every reiteration of all models this number is estimated to reoccur, thus when all models update once another \$285 million in compliance costs will be incurred.

ETA Comments - MD SB 936 AI.pdf

Uploaded by: Claire Hebert

Position: UNF

February 27, 2025

**The Honorable Pamela Beidle
Chair of Senate Finance Committee
Maryland Senate
3 East Miller Senate Office Building
Annapolis, Maryland 21401**

RE: Opposition to SB 936 – Artificial Intelligence

Chair Beidle, Vice Chair Hayes, and Distinguished Members of the Committee,

On behalf of the Electronic Transactions Association (ETA), the leading trade association representing the payments industry, thank you for the opportunity to outline some of our concerns over SB 936. ETA and its members are supportive of efforts to promote responsible use of artificial intelligence (AI) tools and systems. Our industry has long been at the forefront of developing and implementing safeguards to ensure AI is used responsibly and does not result in unjustified differential treatment. ETA's members and their use of AI occurs within the confines of one of the most highly regulated industries, while adhering to the principles of explainability, privacy, risk management, and fairness within existing legal frameworks.

Summary of Specific Feedback:

Implementation: As safeguarding the use of AI is of the utmost importance, ETA and its members believe that updating the effective date from 2025 to 2026 would provide companies more time to come into compliance and to accurately and thoroughly assess their systems.

Removal of Financial Services from a “Consequential decision”: Currently, the list of activities in the definition of consequential decisions uses the term (4) “financial or lending service,” which ETA believes is overbroad and is likely to include low risk AI uses that greatly benefit consumers. Therefore, ETA believes that financial services should be removed from the list of consequential decisions. Doing so will enable companies to take a risk-based approach, consistent with multiple sections of this legislation, and avoid burdensome requirements for low-risk AI uses, such as using AI to categorize expenses for tax or other financial planning purposes or connecting people to financial experts. It will also avoid redundancies because our members already adhere to strict state and federal regulations.

- The inclusion of “a financial service” as consequential could include very low risk AI activity. For example:
 - Categorizing expenses for tax or other financial planning/budgeting purposes.

- Connecting people to financial experts based on the consumers financial/tax needs and the expert's areas of expertise.
- Reading and extracting data from financial forms so consumers don't have to enter data and minimize manual entry errors.
- Recommending financial products like credit cards that may be a good fit for consumers to consider.
- As an alternative, ETA suggests replacing “**a financial service**” with “**a consumer lending decision.**”

High-Risk Artificial Intelligence

Focus on Fraud Protection: ETA appreciates the exclusion of “Anti-fraud technology...” and additional cyber security measures, as AI is an efficient and effective tool at preventing and stopping financial crimes. ETA respectfully requests removing “that does not use facial recognition” to clarify that all anti-fraud technology be included in this exemption to ensure the safety and security of payments.

Deployer Duties

Impact Assessments: Section III requires companies to disclose the data used to customize a model and disclose the cyber security and post-deployment monitoring protocols. While ETA understands these efforts are crucial to safeguarding AI use, the disclosure of such procedures increases the likelihood of bad actors targeting certain dataset types (e.g., financial information), which could result in a multitude of phishing and social engineering attacks. Additionally, if the reports fall into the wrong hands, it could allow bad actors to develop methods of avoiding the detection and protection systems outlined in the report, thus presenting a serious cyber security risk to the company and the end user.

- ETA recommends striking “disclose the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses” as it would be incredibly difficult and burdensome to meet this requirement, and reasonable testing already ensures proper use.
- **Additional Provisions:** A provision included in the Colorado AI law (“CAIA”) provides consideration for impact assessments satisfying the requirement if conducted in accordance with other laws or are similar in scope and effect to the original impact assessment. One impact assessment may cover “a comparable set” of deployed systems, and an assessment completed for complying with another law or regulation can satisfy the requirements of the CAIA if that other assessment “is reasonably similar in scope and effect” to the one required under the CAIA (Sec. 6-1-1703 (3)(d) & (e)). ETA respectfully requests that this consideration be added to this section to avoid duplicating efforts.
- ETA appreciates the rebuttable presumption included under Section 14–47A–03 and requests that this rebuttable presumption also be clarified to include creation of the impact assessments.

As ETA and its members operate in highly regulated industries, ETA respectfully requests adding the following exemption, which was included in Colorado Law:

- “The obligations imposed on developers or deployers by this chapter shall be deemed satisfied for any bank, out-of-state bank, credit union, federal credit union, out-of-state credit union, or any affiliate or subsidiary thereof if such bank, out-of-state bank, credit union, federal credit union, out-of-state credit union, or affiliate or subsidiary is subject to examination by any state or federal prudential regulator under any published guidance or regulations that apply to the use of high-risk artificial intelligence systems.”

Risk Identification

Speculation About Risks: Section 14–47A–03 (A) requests that developers develop a risk management plan for “known or reasonably foreseeable risks of algorithmic discrimination.” Although ETA supports efforts to mitigate the most significant risks of AI, this section presents considerable challenges, including:

- Creating a heavy burden on companies that use AI tools to make long-term predictions about their models’ capabilities before models are trained or built.
- It introduces a vague concept of “reasonableness,” which, while potentially empowering developers to assess whether a model qualifies for an exemption, also carries the risk of ambiguity, and may prove challenging to adhere to without additional insights from industry experts.
- **Liability:** ETA believes that risk and liability should flow with the actor and user in question, rather than remaining with the developer. Therefore, we encourage the use of additional protections for developers in this space to avoid placing regulatory and liability burdens on AI startups.

Attorney General Enforcement (Section 551.105)

- **Timeline:** ETA is grateful for the opportunity to cure, as we believe it supports our shared goals of promoting responsible uses of AI. Similar to the timeline for new impact assessments, allowing companies 90 days for the right to cure any suspected or discovered negative impacts of the use of AI, will allow companies more time to investigate the source of any discrimination and implement meaningful changes.
- Additionally, ETA requests clarification on metrics or parameters outlined in the violation letter to ensure proper curative steps are taken and/or clear showing of thresholds for how the fine amount is to be determined.

Consumer Rights and Remedies

Right of Action: ETA and its members strictly adhere to existing legal and regulatory frameworks, such as the Maryland Personal Information Protection Act (PIPA), which substantively cover a data-subject's rights within the State of Maryland in a manner that would allow end-consumers to enforce data rights against AI use cases without requiring additional legislation. The right of action properly belongs to the AG in those instances as the AG is best situated to bring action against a company for violation.

Privacy & Data: ETA respectfully submits that this legislation could align this section to existing rights and remedies, continuing to allow the state privacy enforcement to bring cases, as they are best equipped to handle cases of this nature due to the sensitivity of the data and information. Consumers have an existing right to correct their personal data under privacy laws, which does not need to be duplicated here.

Customer Appeal: With the alteration of “a financial service” to “a consumer lending decision” within “consequential decision,” consumers already have the right to appeal decisions, with clear and established procedures and courses of action. In general, the ability to appeal could be abused by fraudsters attempting to circumvent or manipulate AI models. An appeal through a human is also not a practical alternative for payments companies, as it undermines the ability to provide credit offers, and humans cannot replace certain tasks, such as determining a credit score.

We appreciate you taking the time to consider these prominent issues. If you have any questions or wish to discuss any aspect of our comments, please contact me.

Respectfully,



Brian Yates
Senior Director, State Government Relations
Electronic Transactions Association
202.677.7417 | byates@electran.org

SB 936_MDCC_Consumer Protection - High-Risk Artifi

Uploaded by: Hannah Allen

Position: UNF



Senate Bill 936

Date: February 27, 2025

Committee: Senate Finance

Position: Unfavorable

Founded in 1968, the Maryland Chamber of Commerce (Maryland Chamber) is a statewide coalition of more than 7,000 members and federated partners working to develop and promote strong public policy that ensures sustained economic growth and opportunity for all Marylanders.

As introduced, Senate Bill 936 (SB 936) aims to protect consumers from algorithmic discrimination in high-risk artificial intelligence systems by imposing new disclosure and impact assessment requirements, while also granting authority to the Attorney General to enforce the act.

SB 936 Imposes Burdensome Disclosure Requirements

To comply with SB 936, developers would be required to notify the consumer when an AI system is used to make a consequential decision about them, by providing the purpose of the system, nature of the decision, and information concerning a consumer's right to opt out of the data processing. This requirement creates a significant compliance burden and cost for each system developed, limiting businesses' ability to compete and discouraging AI innovation by making it more expensive to develop new high-risk systems.

Additionally, compliance with this requirement would result in consumers being inundated with disclosures. A large volume of disclosures would overwhelm consumers, leading to "disclosure fatigue." When inundated with frequent notifications, consumers would likely stop reading them altogether, undermining the bill's intent to provide meaningful transparency.

SB 936 Establishes an Unrealistic Compliance Timeline

The bill would require developers of high-risk AI systems to comply by February 1, 2026 – an unreasonably short timeframe for businesses to update their technology and compliance processes and capabilities. This rushed implementation increases the risk of costly and unnecessary legal challenges once the law takes effect.

SB 936 Introduces a Private Right of Action

SB 936 allows consumers to bring a private right of action if the Attorney General does not respond to an administrative complaint within 180 days. Given the extensive disclosure requirements and tight compliance timeline, this provision exposes businesses to potential litigation before they have adequate time to address safety concerns or adjust to the new regulatory framework.

While we appreciate the intent of this legislation, we have concerns about its implementation. The regulation of high-risk AI systems merits further study and collaboration with industry stakeholders to ensure policies are both effective and practical – for both the developer and consumer.

For these reasons, the Maryland Chamber of Commerce respectfully requests an **unfavorable report** on HB 936.



Ext. Comm. - Testimony - 2025 - Maryland SB 936 -

Uploaded by: Joshua Fisher

Position: UNF



February 25, 2025

The Honorable Pam Beidle
Chair, Senate Finance Committee
Maryland Senate
Annapolis, Maryland 21401

RE: Maryland Senate Bill 936 – High-Risk Artificial Intelligence Developer Act
Position: Unfavorable

Chair Beidle:

Alliance for Automotive Innovation¹ appreciates the opportunity to provide feedback on Senate Bill 936, the High-Risk Artificial Intelligence Developer Act. The automotive industry shares the goal of protecting consumers from algorithmic discrimination while embracing the strengths of artificial intelligence.

Alliance for Automotive Innovation represents the full automotive industry, including the manufacturers producing most vehicles sold in the U.S., equipment suppliers, battery producers, semiconductor makers, technology companies, and autonomous vehicle developers. Our mission is to work with policymakers to realize a cleaner, safer, and smarter transportation future and to ensure a healthy and competitive auto industry that supports U.S. economic and national security. Representing approximately 5 percent of the country's GDP, responsible for supporting 10 million jobs, and driving \$1.2 trillion in annual economic activity, the automotive industry is the nation's largest manufacturing sector.

The automotive industry leverages the power of artificial intelligence to integrate driver support features, advanced safety technologies, and automated driving systems into consumer vehicles. For example, artificial intelligence helps vehicle safety systems understand camera and sensor data, which enables safety features like emergency braking. These and other technological advances have the potential to improve roadway safety, increase traffic efficiency, reduce serious injuries and deaths, and help protect all road users. For these reasons, the automotive industry supports policies that seek to encourage the responsible development and deployment of artificial intelligence technologies.

However, as introduced, SB 936 raises several challenges. To provide a workable framework that meets the objectives of protecting consumers from algorithmic discrimination, fostering innovation,

¹ From the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers – Alliance for Automotive Innovation represents the full auto industry, a sector supporting 10 million American jobs and five percent of the economy. Active in Washington, D.C. and all 50 states, the association is committed to a cleaner, safer and smarter personal transportation future.
www.autosinnovate.org.

and providing regulatory interoperability for businesses, Alliance for Automotive Innovation recommends the following changes:

Definitions

- Revise definition of “consequential decision” to remove references to “access,” which is not defined and not included in similar laws like in Colorado.

Proposed revision to §14-47A-01 (D): “‘Consequential decision’ means a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of: (1) parole, probation, a pardon, or any other release from incarceration or court supervision; (2) education enrollment or education opportunity; (3) financial or lending services; (4) health care services; (5) housing; (6) insurance; (7) marital status; or (8) legal service.”

- Revise definition of “substantial factor” to ensure that high-risk artificial intelligence systems subject to regulatory oversight are factors that have a significant impact on the final consequential decision.

Proposed revision to §14-47A-01 (O)(1): “‘Substantial factor’ means a factor generated by an artificial intelligence system that is: (I) the principal basis for making a consequential decision; and (II) capable of altering the outcome of the consequential decision.”

Operational Provisions

- Add language to §14-47A-04 to provide that if a deployer completes an impact assessment in accordance with another applicable law or regulation, then it shall satisfy this bill’s requirements.

Proposed addition: “If a deployer completes an impact assessment for the purpose of complying with another applicable law or regulation, then the impact assessment satisfies the requirements established in this section if the impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this section.”

- Modify language in §14-47A-05 (B) to specify that evidentiary privilege is available to developers, deployers, and other persons under both federal and state laws.

Proposed modification to §14-47A-05 (B): “The obligations imposed on developers, deployers, or other persons under this subtitle may not apply when compliance by the developer, deployer, or other person would violate an evidentiary privilege under federal law or the laws of the state.”

Enforcement

- Specify in §14-47A-07 that developers and deployers have a minimum of 60 days to cure potential violations before the Attorney General brings an action. The proposed 45-day time period is too short.

Proposed change to §14-47A-07 (C)(2): “If it is possible to cure the violation, the Attorney General may issue a notice of violation to the developer or deployer and afford the developer or deployer the opportunity to cure the violation within 60 days after the receipt of the notice of violation.

Proposed change to §14-47A-07 (C)(4): “If a developer or deployer fails to cure a violation within 60 days after the receipt of a notice of violation under paragraph (3) of this subsection, the Attorney General may proceed with the action.”

- Remove §14-47A-08 because having a private right of action in such a complicated and evolving space would chill innovation. Consumers remain protected because the Attorney General retains enforcement authority under the bill. In addition, consumers can pursue other theories of liability based on common law and statutes (e.g., product liability, consumer protection, etc.), as well as submit complaints to the Attorney General.

Effective Date

- Modify the proposed Act’s effective date to at least October 1, 2026, to allow sufficient time for businesses to align their internal processes and mechanisms with any new regulatory requirements.

Cultivating public trust and transparency in the use of artificial intelligence systems remains critically important to Alliance for Automotive Innovation and its member companies. We appreciate the opportunity to provide this feedback and input and look forward to continuing to work with you on this important topic.

Thank you for your consideration of our position. For more information, please contact our local representative, Bill Kress, at (410) 375-8548.

Sincerely,



Josh Fisher
Senior Director, Alliance for Automotive Innovation

v3_SB 936_compAI_TechNet.pdf

Uploaded by: margaret durkin

Position: UNF



TECHNET
THE VOICE OF THE
INNOVATION ECONOMY

TechNet Mid-Atlantic | Telephone 717.585.8622
www.technet.org | @TechNetMidAtla1

February 25, 2025

The Honorable Pam Beidle
Chair
Senate Finance Committee
Maryland Senate
3 East Miller Senate Office Building
11 Bladen Street, Annapolis, MD 21401

RE: SB 936 (Hester) - Consumer Protection - High-Risk Artificial Intelligence - Developer and Deployer Requirements – Unfavorable

Dear Chair Beidle and Members of the Committee,

On behalf of TechNet, I'm writing to share remarks on SB 936 related to high-risk artificial intelligence.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance. TechNet has offices in Austin, Boston, Chicago, Denver, Harrisburg, Olympia, Sacramento, Silicon Valley, Tallahassee, and Washington, D.C.

Artificial intelligence (AI), machine learning (ML), and the algorithms that often support artificial intelligence have generated policymaker interest. We acknowledge that as technological advances emerge, policymakers' understanding of how these technologies work is vital for responsible policymaking. Our member companies are committed to responsible AI development and use. TechNet will advocate for a federal AI framework that brings uniformity to all Americans regardless of where they live, encourages innovation, and ensures that consumers are protected.

Thank you for allowing TechNet the opportunity to share comments on this bill. We represent a diverse set of members who operate in different AI spaces with different functions. Below are concerns and suggestions we've been made aware of on SB 936 as currently drafted. Additionally, TechNet is supportive of AI workgroups and task forces as they allow for thoughtful deliberation on complex issues. Earlier this month, TechNet was pleased to support enabling legislation in

the Maryland House that would establish a workgroup on artificial intelligence innovation. We believe that a workgroup is the best first step when addressing AI regulation in the states.

Thank you again for the opportunity to comment on SB 936.

Sincerely,

Margaret Durkin

Margaret Durkin
TechNet Executive Director, Pennsylvania & the Mid-Atlantic

TechNet Comments

14-47A-01. – Definitions

“Algorithmic Discrimination” – We’re requesting the sponsor amend this definition to clarify that the bill’s obligations tie back to current anti-discrimination laws.

“Unlawful differential treatment or impact” is a vague concept that will be challenging for businesses to comply with, while actions that violate anti-discrimination laws are well understood. This ensures that existing non-discrimination protections can be applied in a manner that is easily understood by all stakeholders and supported by the current body of state and federal anti-discrimination law. We request the following language instead:

- **“Algorithmic discrimination” means the use of an artificial intelligence system that violates state or federal anti-discrimination laws, including federal statutes prohibiting discrimination on the basis of race, color, sex, disability, religion, familial status, national origin, or citizenship status.**

“Consequential Decision” - We request that the sponsor limit financial services to credit-related services. Suggested language includes striking **“financial or lending services”** and inserting **LOANS FROM A LENDING SERVICE AND DOES NOT INCLUDE FRAUD DETECTION OR FRAUD DETERRENT TECHNOLOGY.**

Or, on page 3, line 29, please consider changing **“financial or lending services”** to **a lending decision**. On Page 3, line 28, please strike **“or provision of”**, and on page 3, line 30, please strike **“or the provision of”**.

“Developer” – In this definition, TechNet requests the sponsor replaces **“offered, sold, leased, given, or otherwise provided to consumers in the state”** with the language: **MADE AVAILABLE FOR USE IN THE STATE.**

“Intentional and substantial modification” – We’re requesting the phrase **AND MATERIAL** after the word **“deliberate”**. Additionally, we believe that any intentional and substantial modification should be reflective of new material risks, rather than reasonably foreseeable ones. Further, the current definition

concerningly still includes a reference to AI models despite the focus again being on high-risk AI systems, and it is not clear what the intent is in clause (ii).

Specifically, the inclusion of clause (ii) is concerning and technically confusing as changing the purpose of a general purpose AI model would mean it is no longer a general purpose model and outside the scope of this bill. We request the sponsor strike (L)(1)(II) on page 6, lines 19-20.

“Substantial Factor” – On page 7, line 27-28, we request striking **“generated by an artificial intelligence system”**. Also on page 7, at line 30, we request replacing the **or** with an **“and”**. On page 8, after line 2, add:

- **and (iii) generated by an artificial intelligence system.**

“Synthetic content” – We request the sponsor amend this definition and suggested language is below.

- “Synthetic content” means information, such as images, video, audio, clips, and text, **content** that has been significantly modified or generated by algorithms, including by artificial intelligence.

14-47A-02 – Exemptions

On page 8, line 22, we’re requesting the following changes. These edits are intended to avoid duplication of regulatory oversight and inconsistencies

(2) AN INSURER, ~~OR~~ **AN INSURANCE PRODUCER LICENSED BY THE STATE**, OR A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM DEVELOPED FOR OR DEPLOYED **BY OR ON BEHALF OF AN INSURER OR AN INSURANCE PRODUCER** FOR USE IN THE BUSINESS OF INSURANCE, IF THE INSURER OR INSURANCE PRODUCER IS SUBJECT TO THE JURISDICTION OF ~~OR REGULATED AND SUPERVISED BY THE~~ INSURANCE ADMINISTRATION **AND SUBJECT TO** ~~AND SUBJECT TO THE PROVISIONS UNDER TITLE 13 OF THIS ARTICLE; EXAMINATION BY SUCH ENTITY UNDER ANY EXISTING STATUTES, RULES, OR REGULATIONS;~~ OR

On page 9, line 6, after **“services”** we request the addition of **TO OR FOR A HEALTHCARE ENTITY** before “using”.

Additionally, we request the following additional exemptions:

(X) A REGULATED ENTITY SUBJECT TO THE SUPERVISION AND REGULATION OF EITHER THE FEDERAL HOUSING FINANCE AGENCY;

The obligations imposed on developers or deployers by this chapter shall be deemed satisfied for any bank, out-of-state bank, credit union, federal credit union, mortgage lender, out-of-state credit union, savings institution, or any affiliate, or subsidiary , or service provider thereof if such bank, out-of-state bank, credit union, federal credit union, mortgage

lender, out-of-state credit union, savings institution, or affiliate, or subsidiary, or service provider is subject to the jurisdiction of any state or federal regulator under any published guidance or regulations that apply to the use of high-risk artificial intelligence systems and such guidance or regulations.

14-47A-03. – Developers

On page 9, line 12, we request that **material** be added after “foreseeable”.

At (3) (V), replace “should” with **IS INTENDED TO**.

And add **BASED ON KNOWN HARMFUL OR INAPPROPRIATE APPLICATIONS** after the phrase “**not be used**”. This would clarify the reporting and documentation requirement to specify that the developer is responsible for providing documentation describing how a high-risk artificial intelligence system should not be used based on known harmful or inappropriate applications.

Regarding documentation requirements, we believe that these requirements are broad and loop in AI models and “dataset card files”. This provision needs to be narrowed to only require relevant impact assessments. We propose that the sponsor strike lines 16-23 on page 11 and insert for new (I) “**the artifacts including system cards or predeployment impact assessments, including any risk management policy designed and implemented and any relevant impact assessment completed**”.

On page 12, line 13, we request striking “**and at least as stringent as**”. This is very subjective standard that will be difficult for compliance purposes. “Substantially equivalent to” is enough to ensure they are aligned with the listed frameworks.

Our members remain concerned about the obligations to mark synthetic content as they believe it’s technically infeasible at this time. As written, the bill applies the synthetic marking requirements to all generative AI systems; however, it seems this may be a drafting error as the provision also references high-risk AI systems. The bill is otherwise tailored to high-risk AI applications and this provision should take the same approach. Tailored changes are needed to clarify the scope of the synthetic marking requirements. We suggest the following changes in (G)(1):

- On page 12, line 24, add **high-risk** before “**generative**” and strike “**or modifies**” on line 25.

14-47A-04. – Deployers

In (A)(1), we’re requesting the sponsor align that language with the language in the developer section. Specifically, by adding in language **of a high-risk artificial intelligence system**. Additionally, we request the word **material** be added after “foreseeable” on page 13, line 25.

On the risk management section, on page 14, line 3, please strike **"and maintain"**. Also, on page 14 at line 6, strike **"and maintained"**. In addition, please strike lines 13-14. On line 15, strike **"and in consideration of"** and add **"considering"** after **"reasonable"**. Like in the developer section, we request the sponsor strike the phrase **"and at least as stringent as"** on lines 29-30 on page 14. And again, on page 15, lines 10-11.

Regarding the 90-day disclosure update requirement, we believe that the clock should start when a deployer is notified and given information as required by this act. The timeline for such assessments may prove impractical, particularly as the risk of discrimination may not be apparent on its face. We request the following language on page 15, starting at line 18:

- (II) ~~**AT-LEAST WITHIN 90 DAYS BEFORE-OF BEING NOTIFIED BY THE DEVELOPER THAT**~~ A SIGNIFICANT UPDATE TO A HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM IS ~~**MADE**~~ AVAILABLE, A DEPLOYER SHALL COMPLETE AN IMPACT ASSESSMENT OF THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM IF THE UPDATE PRODUCES A NEW VERSION OR RELEASE ~~**OR SIMILAR-CHANGE**~~ TO THE HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEM THAT:

On page 15, line 23, strike **"significant"** and replace it with **"material"**. On page 16, at line 1 and at line 10, strike the phrase **"An analysis of"**. On page 17, line 3, strike **"contemporary social science standards"** and replace with **"standard industry practices"**. Also on page 17, line 28, strike **"will"** and replace with **"is intended to"**. Add **"if any"** after "assess" on line 28, and strike **"and the method by which the system measures or assesses personal characteristics or attributes"**. Without this strike, this provision would require the disclosure of information otherwise protected as s or confidential or proprietary information.

Regarding consumer disclosures, SB 936 goes far beyond the intent to provide an individual notice when a consumer is interacting with an AI system. Such a broad and prescriptive requirement is not risk-based and creates serious concerns about privacy risks. Furthermore, the opt-out provision on page 17 includes a novel requirement. We urge this provision be narrowed to what is required under the Colorado AI Act and strike the reference to an opt-out. We suggest the following language:

- **Disclosures are not required under circumstances in which it would be obvious to a reasonable person that the person is interacting with an artificial intelligence system.**

On page 18, line 3, add **","if any"** after **"system."**

On page 18, strike lines 9-18, and on page 19, strike lines 1-9. TechNet requests this extensive amendment because these disclosure requirements will result in companies providing extensive information that is likely to be confusing and difficult

to understand by consumers. More importantly, the language in the current draft would require the disclosure of confidential and proprietary information, as well as trade secrets that are otherwise protected in the bill. Further, given the current competitive environment, such extensive disclosures run the risk of providing foreign adversaries with detailed information about American-developed AI systems that can be used to advance their position in the global marketplace, harming American interests. As such, we request deleting the entire subsection.

On adverse decisions, this bill doesn't include **"technically reasonable and practicable"** language for allowing human review, and it provides an overly prescriptive requirement for how such information should be provided to users. We urge the inclusion of this needed flexibility for compliance. We request the sponsor strike 14-47A-04(F).

To align with the Developer section, please add the following trade secret language:

- (X) THAT IS A TRADE SECRET, AS DEFINED IN § 11-1201 OF THIS ARTICLE, OR OTHERWISE PROTECTED FROM DISCLOSURE UNDER STATE OR FEDERAL LAW; OR**
- (X) THE DISCLOSURE OF WHICH WOULD:**
 - (X) PRESENT A SECURITY RISK TO THE DEPLOYER; OR**
 - (XX) REQUIRE THE DEPLOYER TO DISCLOSE CONFIDENTIAL OR PROPRIETARY INFORMATION.**

Cure Period

We appreciate the sponsor including the right to cure provisions in this bill; however, we prefer that a cure option is always included, rather than be at the discretion of the Attorney General. Additionally, we're requesting that any cure period be 90 days. We are also concerned by the inclusion of "any harm" as part of this obligation. This is far too broad and could apply to any potential harm, no matter how minor or unlikely. We recommend that this be tied to "known harms of algorithmic discrimination" to align within the intent of the bill.

Enforcement

We request the sponsor remove language granting the Attorney General the ability to adopt regulations. Additionally, we request amendments to the affirmative defense requirements to allow for other methods than only red-teaming. Finally, we are requesting the private right of action (PRA) be removed from this legislation. It's our belief that PRAs lead to frivolous lawsuits that don't derive real value for consumers, and that enforcement should rest solely with the Attorney General.

SB0936 - MBA - INF - GR25.pdf

Uploaded by: Evan Richards

Position: INFO



**SB 936 – Consumer Protection - High-Risk Artificial Intelligence -
Developer and Deployer Requirements
Committee: Senate Finance Committee
Date: February 27, 2025
Position: Letter of Information**

The Maryland Bankers Association (MBA) appreciates the opportunity to provide informational testimony on SB 936 and how it impacts Maryland's banking industry. MBA hopes that the Senate Finance Committee, instead of passing SB 936 this session, will consider taking additional time to examine artificial intelligence (AI) regulation and consider legislation in future years that includes feedback from industries that use AI to improve the lives of Marylanders.

Maryland banks use AI to streamline operations, enhance customer experience, and improve fraud detection. They do so in compliance with state and federal lending laws to ensure transparency, accountability, and non-discrimination. Bank regulators consistently review a bank's use of AI during examinations. Regulators can request documentation and review algorithms to ensure that models align with regulatory guidelines. Failure to comply with regulatory guidelines that prohibit discrimination can result in penalties ranging from fines to legal action. Banks never want to run afoul of their regulators, so a strong incentive to use AI in a transparent and compliant fashion already exists.

While it is unclear whether all of SB 936 would apply to Maryland banks, it is important to take into consideration how the requirements of this bill may either be redundant or contradict existing AI requirements for Maryland banks. Accordingly, the MBA urges the Senate Finance Committee to continue studying the use of AI to produce a legislative product that does not stifle innovation and would not put Maryland banks into a situation where they run afoul of federal laws and regulations. MBA looks forward to being a part of conversations around the regulation of AI in the coming months and years.

The Maryland Bankers Association (MBA) represents FDIC-insured community, regional, and national banks, employing thousands of Marylanders and holding more than \$194 billion in deposits in almost 1,200 branches across our State. The Maryland banking industry serves customers across the State and provides an array of financial services including residential mortgage lending, business banking, estates and trust services, consumer banking, and more.

MD SB 936 ATA Action Letter.pdf

Uploaded by: Hunter Young

Position: INFO



February 25, 2025

The Honorable Pamela Beidle
Senator, Senate District 32
Chair, Maryland Senate Finance Committee
3 East Miller Senate Office Building
Annapolis, MD 21401

RE: ATA Action Comments on [SB 936](#)

Dear Chair Beidle, Chair and members of the Maryland Senate Finance Committee,

On behalf of the ATA Action, I am writing to offer feedback on SB 936, the High-Risk Artificial Intelligence Developer Act. ATA Action appreciates the work that stakeholders have done thus far on this bill and write specifically with comments on the bill's provision regarding use of AI in delivering or administering healthcare services.

ATA Action, the American Telemedicine Association's affiliated trade association focused on advocacy, advances policy to ensure all individuals have permanent access to telehealth services across the care continuum. ATA Action supports the enactment of state and federal telehealth policies to secure telehealth access for all Americans, including those in rural and underserved communities. ATA Action recognizes that telehealth and virtual care have the potential to truly transform the health care delivery system – by improving patient outcomes, enhancing safety and effectiveness of care, addressing health disparities, and reducing costs – if only allowed to flourish.

As artificial intelligence (AI) has continued to become more refined, healthcare entities have begun to utilize this technology in many aspects of care delivery due to its potential to improve quality and service capacity at every state of the care journey. AI-powered technologies are being deployed to analyze data quickly and accurately to assist providers in making better informed decisions and identifying diseases earlier. AI is also helping healthcare entities streamline administrative tasks-- such as improving patient scheduling or medication refill requests--which frees up more time for patient care. Accordingly, legislators and regulators have begun to consider the proper guardrails for the use of AI in healthcare, allowing for increased innovation and efficiency while ensuring patient care is not compromised. With this in mind, last year the ATA adopted [AI Principles](#) to help guide policies that enhance patient and provider trust, safety, and efficacy of AI adoption as a tool in healthcare, including in telehealth.

Section 14-47A-02(3) of SB 936 makes clear that the bill's provisions do not apply to HIPAA covered entities providing (I) providing healthcare recommendations through AI that require a provider to implement those recommendations and (II) using AI powered services for administrative, financial, quality measurement, security, or performance improvement functions. ATA Action appreciates and supports this exemption. Indeed, health care entities—and the technology partners and vendors they work with—already must follow a number of complex federal and state frameworks that address the intent of SB 936. This exemption avoids HIPAA covered entities from being subject to additional, duplicative, and potentially inconsistent regulation, which creates unnecessary and inappropriate burdens and cost. Further, many of the bill's provisions could be difficult to operationalize in healthcare settings, where AI powered tools are often embedded into clinical workflows.

ATA ACTION

901 N. Glebe Road, Ste 850 | Arlington, VA 22203
Info@ataaction.org



While we support the exemption, ATA Action believes it must also include those non-HIPAA covered entities providing or supporting healthcare services, such as Maryland licensed healthcare providers that do not take insurance and the third-party services providers perform functions on their behalf. As currently drafted, the bill will subject Maryland healthcare providers and entities to two different standards without justification. In some cases, the same health care provider could be subject to two different statutory regimes based on the patients' forms of payment for services received. Moreover, low cost telehealth providers that are not HIPAA covered likely will be subject to additional administrative hurdles just to obtain or use AI-powered software, making these innovation solutions more expensive (at a minimum) and potentially unavailable. To resolve this issue, we recommend adding the following amendment to Section 14-471-02(3):

The provisions of this chapter shall not apply to a developer, integrator, distributor, deployer, or other person that ~~is a covered entity within the meaning of the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d et seq.) and the regulations promulgated under such federal act, as both may be amended from time to time,~~ and is providing (i) health care recommendations that (a) are generated by an artificial intelligence system and (b) require a health care provider to take action to implement the recommendations or (ii) services to or for a healthcare entity using an artificial intelligence system for an administrative, financial, quality measurement, security, or performance improvement function.

ATA Action hopes you will favorably consider and adopt these changes. Thank you for your support of telemedicine. We encourage you and your colleagues to consider amendments to SB 936 to ensure easy and efficient access to high-quality health care services in Maryland.

Please do not hesitate to let us know how we can be helpful to your efforts to advance common-sense telemedicine policy. If you have any questions or would like to discuss the telemedicine industry's perspective further, please contact me at kzebley@ataaction.org.

Kind regards,

Kyle Zebley
Executive Director
ATA Action

MMHA - 2025 - SB936 - INF.pdf

Uploaded by: Matthew Pipkin

Position: INFO



Senate Bill 936

Committee: Finance

Bill: Senate Bill 936 – Consumer Protection - High-Risk Artificial Intelligence - Developer and Deployer Requirements

Date: 2/27/25

Position: Informational

The Maryland Multi-Housing Association (MMHA) is a professional trade association established in 1996, whose members house more than 538,000 residents of the State of Maryland. MMHA's membership consists of owners and managers of more than 210,000 rental housing homes in over 958 apartment communities and more than 250 associate member companies who supply goods and services to the multi-housing industry.

Senate Bill 936 ("SB 936") requires a certain developer of, and a certain deployer who uses, a certain high-risk artificial intelligence system to use reasonable care to protect consumers from known and reasonably foreseeable risks of certain algorithmic discrimination in a certain high-risk artificial intelligence system. Additionally, SB 936 regulates the use of high-risk artificial intelligence systems by establishing certain requirements for disclosures, impact assessments, and other consumer protection provisions. SB 936 would also allow the Office of the Attorney General to enforce the Act and create regulations.

On page 4 line 1, SB936 includes "HOUSING" in its list of consequential decisions that would be subjected to this legislation. Given the new and developing nature of the use of artificial intelligence in the housing industry, MMHA is currently engaging with membership and stakeholders to review this legislation for potential impacts. The immediate concerns stem from housing providers' ability to conduct credit screenings, tenant selections, and utilize pricing tools with industry standard devices.

Several initial questions have been raised by members regarding this legislation:

- Would credit scoring models qualify as a "high-risk artificial intelligence systems" and be subjected to this legislation?
- How would the Office of the Attorney General intend to enforce and establish regulations? Do they have existing resources to act in this capacity? To our knowledge, this would be the first instance of direct regulatory authority coming from the OAG.
- How exactly would developers test for bias based on the list of protected classes in bill?

Additionally, a few general concerns have also been raised:

- **Technological Challenges:** Ensuring that AI systems are free from algorithmic discrimination and bias can be technically challenging. Developers of the AI systems may need to invest in advanced technologies and expertise to meet these requirements.

- **Compliance Costs:** Implementing the required changes to ensure AI systems are fair and non-discriminatory may involve significant costs. This includes updating algorithms and conducting regular impact assessments.
- **Operational Adjustments:** The need for regular impact assessments and detailed disclosures may require changes to existing workflows and processes. This could lead to increased administrative burdens and the need for additional staff or resources.
- **Legal and Regulatory Risks:** Non-compliance with the bill's requirements could result in legal and regulatory penalties.

MMHA is still eliciting feedback from the housing industry on this legislation, and therefore will defer our position on SB936 to informational at this time. We look forward to engaging with the sponsors and other stakeholders of the legislation to address our questions and concerns.

Please contact Matthew Pipkin, Jr. at (443) 995-4342 or mpipkin@mmhaonline.org with any questions.