Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

Technology, Economic Development, & Veterans Committee

HB 2157

Brief Description: Regulating high-risk artificial intelligence system development, deployment, and use.

Sponsors: Representatives Ryu, Stearns, Ramel, Parshley and Reeves.

Brief Summary of Bill

- Establishes that developers and deployers of high-risk artificial intelligence (AI) systems are required to use reasonable care to protect consumers from algorithmic discrimination.
- Establishes requirements for developers and deployers of high-risk AI systems relating to transparency and risk management.

Hearing Date: 1/14/26

Staff: Emily Poole (786-7106).

Background:

Artificial intelligence (AI) is defined and understood in different ways. The National Institute of Standards and Technology, in its AI Risk Management Framework, defines an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments.

In 2024 the Legislature established the AI Task Force, administered by the Office of the Attorney General. The Task Force is tasked with assessing current uses and trends of AI and making recommendations to the Legislature regarding guidelines and potential legislation for the

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

use of AI systems.

Summary of Bill:

Operating Standards for Developers of High-Risk AI Systems.
A developer of a high-risk AI system is required to use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the AI system.

Subject to certain exceptions, a developer may not provide a high-risk AI system to a deployer or other developer unless the developer makes available:

- a statement disclosing the intended uses of the system;
- documentation disclosing certain information, including: the known or reasonably known limitations of the system; the purpose of the system and its intended outputs, benefits, and uses; a summary describing how the system was evaluated for performance and for mitigation of algorithmic discrimination; and a description of how the system should be monitored when used to make a consequential decision; and
- any additional documentation that is reasonably necessary to assist the deployer or other developer in understanding the outputs and in monitoring for risks of algorithmic discrimination.

A developer that makes a high-risk AI system available to a deployer or other developer is required to also make available certain information to enable the deployer, other developer, or a third-party contractor to complete required impact assessments.

Subject to certain exceptions, a developer of a high-risk generative AI system must ensure that the outputs of such system: (1) are identifiable and detectable in an accessible manner; (2) comply with applicable accessibility requirements; and (3) apply such identification at the time the output is generated.

Operating Standards for Deployers of High-Risk AI Systems.
A deployer of a high-risk AI system is required to use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination.

A deployer may not deploy a high-risk AI system to make a consequential decision unless the deployer has implemented a risk management policy and program. Subject to certain exceptions, a deployer that uses a high-risk AI system to make a consequential decision must have also completed an impact assessment. The impact assessment must include certain required contents, including information about the system's purpose and deployment context, the risks of algorithmic discrimination, the intended use cases, the system's inputs and outputs, system customizations, performance metrics, transparency measures, monitoring and safeguards, and the system's validity and reliability, among other information.

At or before the time that a deployer uses a high-risk AI system to interact with a consumer, the

deployer is required to disclose to the consumer that the consumer is interacting with an AI system. The disclosure must include certain other information, including the purpose and nature of the system, the nature of the consequential decision, deployer contact information, and a description of the AI system in plain language.

A deployer that uses a high-risk AI system to make a consequential decision must send the decision to the consumer without undue delay. If the decision is adverse to the consumer and based on personal data beyond information that the consumer provided, the deployer must disclose the principal reasons for the decision, including the degree to which the high-risk AI system contributed to the decision.

A deployer is required to make available a summary of how the deployer manages reasonably foreseeable risks of algorithmic discrimination that may arise from the use of the high-risk AI system.

Exceptions.
Several exemptions are established, including for certain AI systems that are acquired by or for the federal government. Other exempt entities include regulated financial institutions, certain insurers, and certain health care entities, among other entities.

Compliance with Risk Management Frameworks.
High-risk AI systems that are in conformity with certain national or international AI risk management frameworks are presumed to be in compliance with applicable requirements for developers and deployers. In addition, a deployer's risk management policy and program are presumed to be in compliance with applicable requirements if they align with certain national or international AI risk management frameworks.

Enforcement.
A person may file a civil action against a developer or deployer for a violation of the bill's requirements. In such an action, there is a rebuttable presumption that a developer or deployer of a high-risk AI system used reasonable care if the developer or deployer was in compliance with applicable requirements.

If a court finds that the developer or deployer violated applicable requirements, the court may enjoin the violation and award reasonable attorneys' fees and costs. It is an affirmative defense that the developer or deployer: discovered a violation; cured the violation within 45 days; provided notice and evidence to the person bringing the civil action that the violation has been cured; and is otherwise in compliance with applicable requirements.

Definitions.
Several terms are defined, including "algorithmic discrimination," "consequential decision," and "high-risk artificial intelligence system," among others.

Appropriation: None.

Fiscal Note: Requested on January 6, 2026.

Effective Date: The bill takes effect on January 1, 2027.