R Street
Free markets. Real solutions.

EXPLAINER

Federal Artificial Intelligence Risk Management Act of 2023/2024

S.3205/H.R. 6936

Cybersecurity Legislative Analysis Series

Bill Summary: Establishes guidelines to be used within the federal government to mitigate risks associated with artificial intelligence (AI).

Referred to Senate Committee on Homeland Security and Governmental Affairs/House Committee on Oversight and Accountability, and House Committee on Science, Space, and Technology.

Rating: CYBER POSITIVE This bill has the potential to improve the safety and security of AI technologies deployed within the federal government.

Status: S.3205/H.R.6936—Federal Artificial Intelligence Risk Management Act of 2023/2024

Last updated: Feb. 22, 2024

Key Provisions

- Requires the Office of Management and Budget (OMB) to direct federal agencies to adopt the Artificial Intelligence Risk Management Framework (RMF) developed by the National Institute of Standards and Technology (NIST) regarding the use of AI
- Specifies appropriate cybersecurity strategies and the installation of effective cybersecurity tools to improve the security of AI systems
- Establishes an initiative to deepen AI expertise among the federal workforce
- Ensures that federal agencies procure AI systems that comply with the framework
- Requires NIST to develop sufficient test, evaluation, verification, and validation capabilities for AI acquisitions

Background

Federal agencies employ AI systems for a range of purposes, from addressing cybersecurity vulnerabilities to automating redundant processes to improving health care outcomes. However, with the adoption of novel technology and no universally enforced standards for its safety and security, the federal government's use of that technology is susceptible to challenges and risks, including:

- How to best mitigate data privacy and security risks associated with data collected and processed on Americans;
- How to address challenges associated with the lack of transparency about AI decision-making; and
- Reducing or eliminating potential negative outcomes as a result of the use of untrue or unverified data.

In 2023, NIST released its first iteration of the AI RMF, a set of voluntary best practices that individuals, organizations, and society can use to better manage risks associated with AI. The RMF has two primary components. The first frames AI risks and discusses the characteristics of trustworthy AI systems: valid and reliable; safe; secure and resilient; accountable and transparent; explainable and interpretable; privacy-enhanced; and fair with their harmful bias managed. The second component describes four specific functions to address the risk of AI systems. The RMF has been praised for being a "rights-preserving, non-sector specific," and adaptable framework for all types and sizes of organizations; the framework is also interoperable with international standards.

Background

(continued)

Given the opaqueness of some AI systems and the potential inconsistencies in outputs, risks posed by AI are unique. The NIST AI RMF provides a structured methodology for ensuring that organizations can formulate internal processes and tools to address risks that have the potential to introduce harm. President Joe Biden's 2023 Executive Order (EO) 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence sought to incorporate the AI RMF into federal agencies' guidelines and best practices (sections 4.1(a)(i)(A) and 4.3 (a)(iii)), and to promote the AI RMF as a worthy global technical standard (sections 11(b) and 11(c)).

Key Takeaways

A legislative approach can encapsulate and give statutory support to some of the directives outlined in President Biden's EO and avoid some typical pitfalls of EOs (e.g., the risk of a future administration rescinding components (or the entirety) of the EO, or executive branch overreach concerns). These bills being a bipartisan, bicameral effort indicates that there is broad consensus around its merits and that political will exists for its passage. It would also mark one of the first times where adoption or use of NIST frameworks would be required for the federal government and private sector vendors. In particular, these bills would have a number of improvements for AI security and cybersecurity, including:

- Suppliers attesting compliance to the RMF in order to be eligible for a federal AI contract award;
- Raising public sector resilience against AI misuse and risks and improving harmonization of technical and security standards across federal agencies; and
- Consistent engagement, review, and updating of standards for the test, evaluation, verification, and validation of AI acquisitions.

Cybersecurity Analysis

FACTORS	ANALYSIS
Access provisions	The bill language states that suppliers shall provide "appropriate access to data, models, and parameters...to enable sufficient test and evaluation, verification, and validation" as part of the model contract language to be developed.
Applicability	This bill only applies to federal government use and vendors that provide AI or AI-enabled technology to the federal government, with an exemption for "national security systems" (more in Exemptions, below).
Impact on cyber actions	Implementation of an evolving, consensus-based framework has the potential to improve cybersecurity by requiring the adoption of framework principles in both federal agencies and private sector entities that provide services or products that use AI to the federal government.
Business impact	There is a likelihood that current federal government vendors that sell AI technology to the federal government would have to expend resources to develop policies and procedures to comply with the framework. Failure to do so could mean that the vendor becomes ineligible to receive AI-related contract awards. The bill language requires suppliers to adhere to actions that are "consistent with the framework," but does not specify what those actions will be. Smaller organizations and vendors who do not have sufficient resources to comply with the framework may mean that they are unable to compete with larger or better resourced vendors.

Cybersecurity Analysis (continued)

FACTORS	ANALYSIS
Data privacy and data security	The framework as implemented is likely to impose requirements for considerations of data privacy and data security, especially as it pertains to sensitive information (e.g., intellectual property, confidential data) or personal identifiable information. The bill explicitly states that NIST shall provide standards "that are tailored to risks that could endanger people and the planet," and we can assume that data privacy and security fall within that characterization.
Rulemaking or update mechanisms	The OMB will issue guidance for federal agencies to incorporate the framework into their risk management efforts within 180 days of enactment. The Administrator of Federal Procurement Policy and the Federal Acquisition Regulatory Council will ensure federal agencies procure AI systems that incorporate the framework within one year of enactment. Finally, NIST will develop test and evaluation capabilities for AI acquisitions within one year of enactment, and continuously update these standards as voluntary consensus standards also evolve.
Exemptions, exceptions, defenses	National security systems (as defined in section 3552 of title 44, U.S. Code) will be exempted from requirements stipulated in Sec. 2. (b) (2) Requirements for Agency Use of Artificial Intelligence.
Enforcement mechanisms	Enforcement mechanisms are not specified in the bill, but it may fall on the procurement offices dedicated to the acquisition of AI technology.
Other notes	Microsoft, Okta, Workday, IEEE-USA, Hugging Face, the Enterprise Cloud Coalition, and other organizations have endorsed the Senate version of the bill. The House companion bill references the same endorsements.

Recommendations

With the concerns highlighted in our analysis, we offer the following recommendation in an aim to mitigate challenges and reduce risks.

SECTION AND SUMMARY	RECOMMENDATION(S)
Section 2(b)(8) Exception for National Security Systems	Carving a blanket exception for "national security systems" to comply with the NIST AI RMF may be harmful to cybersecurity and national security by waiving a requirement for systems that arguably touch upon sensitive, classified, or proprietary information. **RECOMMENDATION:** Amend this provision to include some internal audit or compliance requirement within agencies focused on national security to comply with best practices and guidelines of the RMF and other relevant frameworks.