.....

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To provide for certain artificial intelligence agent discovery and security standards, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. GOTTHEIMER introduced the following bill; which was referred to the Committee on _____

A BILL

To provide for certain artificial intelligence agent discovery and security standards, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Stop Rogue AI Act''.

SEC. 2. AI AGENT DISCOVERY AND SECURITY STANDARDS.

(a) AI AGENT DISCOVERY AND SECURITY STANDARDS.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act and annually

thereafter, the Director of the National Institute of Standards and Technology (in this section referred to as the ''Director''), in coordination with the Assistant Secretary of Commerce for Communications and Information (in this section referred to as the ''Assistant Secretary''), shall develop, publish, and maintain standards, guidelines, and best practices for the secure development, deployment, and operation of artificial intelligence agents by an organization. Such standards, guidelines, and best practices shall—

(A) maintain the capability to continuously discover, inventory, verify, and maintain organizational control over all AI agents operating within or interacting with the information systems, networks, applications, services, or digital environments of such organizations;

(B) maintain organizational control over AI agents deployed by such organization;

(C) integrate discovery mechanisms into broader cybersecurity and risk management processes, consistent with defense-in-depth;

(D) apply discovery and verification controls consistently across AI agents regardless of whether such AI agents are developed inter-

nally, acquired from third-party vendors, or operated through external services;

(E) evaluate the security, safety, correctness, and reliability of AI agents before such AI agents are deployed by such organization and continuously after such deployment;

(F) enable continuous runtime monitoring and, where appropriate, inline detection and interception of AI agent interactions with tools, data sources, information systems, and other AI agents, including detection of prompt injection, data exfiltration, anomalous tool invocation, and behavioral drift from an AI agent's approved operational baseline;

(G) implement cryptographically verifiable provenance mechanisms sufficient to identify the entity responsible for creating or operating an AI agent; and

(H) generate and retain tamper-evident, standardized logs of material AI agent actions, and ensure such logs are portable and accessible, as appropriate and consistent with law, to deploying organizations and authorized relying parties.

(2) AI AGENT DISCOVERY AS A COMPONENT OF CYBERSECURITY.—In carrying out paragraph (1), the Director, in coordination with the Assistant Secretary, shall include in the standards, guidelines, and best practices described in such paragraph AI agent discovery as a necessary component of effective cybersecurity within applicable frameworks, profiles, and reference materials.

(3) OPEN AND INTEROPERABLE DISCOVERY STANDARDS.—The Director, in coordination with the Assistant Secretary, shall support the development and adoption of open, vendor-agnostic, and interoperable standards for AI agent discovery mechanisms. In carrying out this paragraph, the Director and the Assistant Secretary shall—

(A) promote the use of existing internet infrastructure and identity-based discovery mechanisms, including domain name system-based approaches, cryptographically verifiable AI agent identity and registry frameworks, or functionally equivalent mechanisms, to enable secure and scalable AI agent discovery and AI agent identity verification;

(B) ensure that such standards are globally interoperable, distributed, and not depend-

ent on proprietary or platform-specific registries; and

(C) engage with multistakeholder processes, including industry, civil society, and technical standards bodies, to support broad adoption and international coordination.

(4) MINIMUM ORGANIZATIONAL REQUIREMENTS.—Standards, guidelines, and best practices developed under this subsection shall provide that organizations deploying AI agents—

(A) maintain a continuous, machine-readable inventory of all AI agents, using standardized, vendor-agnostic naming conventions;

(B) implement AI agent identity verification and trust verification mechanisms that are independent and cryptographically verifiable at both the network and application layers; and

(C) do not rely solely on self-attested or single-provider assertions for establishing AI agent identity.

(5) GUIDANCE, COORDINATION, AND DEMONSTRATION PROJECTS.—The Director, in coordination with the Assistant Secretary, shall—

(A) incorporate the standards, guidelines, and best practices developed under this subsection into existing National Institute of Standards and Technology frameworks and guidance;

(B) ensure that standards, guidelines, and best practices developed under this subsection are consistent with and not duplicative of other efforts by National Institute of Standards and Technology to establish standards related to AI agents;

(C) conduct or support demonstration projects, including through the National Cybersecurity Center of Excellence, to evaluate the effectiveness of open agent discovery mechanisms;

(D) coordinate with the Administrator of the National Telecommunications and Information Administration to promote outreach and adoption through multistakeholder processes and international engagement, as appropriate; and

(E) coordinate with the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to en-

sure AI agent discovery standards are reflected in applicable Federal civilian agency security guidance and binding operational directives, as appropriate.

(b) FEDERAL PROCUREMENT REQUIREMENTS FOR AI AGENT SECURITY.—

(1) IN GENERAL.—Not later than 18 months after the publication of standards, guidelines, and best practices under subsection (a) and annually thereafter, the Federal Acquisition Regulatory Council shall propose revisions to the Federal Acquisition Regulation to require contractors and Federal agencies procuring or deploying, as the case may be, AI agents or information systems that interact with AI agents to comply with such standards, guidelines, and best practices.

(2) REQUIRED CONTRACT ELEMENTS.—Revisions proposed under paragraph (1) shall ensure contracts for the procurement or deployment of AI agents include requirements that the contractor—

(A) maintain a continuous, machine-readable inventory of all AI agents deployed under such contract, using standardized, vendor-agnostic naming conventions consistent with

standards, guidelines, and best practices developed under subsection (a);

(B) implement AI agent identity verification mechanisms that are cryptographically verifiable at both the network and application layers;

(C) ensure AI agent discovery and verification capabilities are accessible to the Federal agency that has entered into such a contract without reliance on the contractor with which such Federal agency has so entered into such a contract;

(D) enable the Federal agency that has entered into such a contract to exercise organizational control over AI agent activity, including the ability to allow, deny, or constrain AI agent-to-AI agent and AI agent-to-information system interactions;

(E) enable the Federal agency that has entered into such a contract to provide cryptographically verifiable provenance information to authorized entities interacting with the AI agent, consistent with the policies of such Federal agency; and

(F) generate tamper-evident, standardized logs of material AI agent actions, and ensure such logs are portable and accessible to the Federal agency that has entered into such a contract and, where appropriate and consistent with law and such contract, authorized relying parties.

(3) REQUIRED CONTRACT ELEMENTS FOR INFORMATION SYSTEMS INTERACTING WITH AI AGENTS.—Revisions proposed under paragraph (1) shall ensure contracts for the procurement or deployment of information systems that AI agents interact with include requirements that the contractor—

(A) maintain a continuous, machine-readable inventory of all AI agents that interact with such an information system, using standardized, vendor-agnostic naming conventions consistent with standards, guidelines, and best practices developed under subsection (a);

(B) implement identity verification mechanisms that are cryptographically verifiable for all AI agents that interact with such an information system;

(C) implement provenance verification mechanisms that are cryptographically verifiable for all AI agents that interact with such an information system;

(D) ensure AI agent discovery and verification capabilities are accessible to the Federal agency that has entered into such a contract without reliance on the contractor with which such Federal agency has so entered into such a contract;

(E) enable the Federal agency that has entered into such a contract to exercise organizational control over AI agents' ability to interact with such an information system, including the ability to allow, deny, or constrain AI agent-to-AI agent interactions within such an information system; and

(F) generate tamper-evident, standardized logs of material AI agent actions within such an information system and ensure such logs are portable and accessible to the Federal agency that has entered into such a contract and, where appropriate and consistent with law and such contract, authorized relying parties.

(4) SAVING PROVISION FOR CERTAIN CONTRACTS.—This subsection shall not apply to contracts for the procurement or deployment, as the case may be, of AI agents or information systems that interact with AI agents entered into before the date of the enactment of this Act.

(5) AGENCY GUIDANCE.—Not later than 180 days after the proposal of revisions under paragraph (1) and annually thereafter, the Director of the Office of Management and Budget, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall issue guidance to Federal agencies regarding the following:

(A) The implementation of procurement requirements under this subsection, including for AI agents deployed through cloud services, platform integrations, or third-party managed environments.

(B) The effective usage of AI agents by such Federal agencies in accordance with the standards, guidelines, and best practices under subsection (a).

(c) DEFINITIONS.—In this section:

(1) AI AGENT DISCOVERY.—The term ''AI agent discovery'' means the technical and organiza-

tional capability to identify, enumerate, verify, and maintain a current inventory of AI agents operating within, communicating with, or seeking access to an information system, network, application, service, or digital environment.

(2) AI; ARTIFICIAL INTELLIGENCE.—The terms ''AI'' and ''artificial intelligence'' have the meaning given the term ''artificial intelligence'' in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(3) AI MODEL.—The term ''AI model'' means a software component of an information system that implements artificial intelligence technology and uses computational, statistical, or machine-learning techniques to produce outputs from a defined set of inputs.

(4) ARTIFICIAL INTELLIGENCE AGENT; AI AGENT.—The terms ''artificial intelligence agent'' and ''AI agent'' mean a software-based system that—

(A) uses an AI model to perceive, plan, or make decisions;

(B) autonomously interacts with other software systems, digital services, users, exter-

nal environments, or AI agents on behalf of a person or organization; and

(C) involves minimal or no human interaction beyond its initial direction.

(5) DEFENSE-IN-DEPTH.—The term ''defense-in-depth'' means the protection of information systems by using multiple security measures, including policies, procedures, and physical security, such as antivirus software, firewalls, anti-spyware tools, strong password policies, intrusion detection systems, biometric verification, encryption, and multi-factor authentication, to reduce the risk of unauthorized access, data breach, or other successful attack.

(6) INFORMATION SYSTEM.—The term ''information system'' has the meaning given such term in section 3502 of title 44, United States Code.

(7) ORGANIZATIONAL CONTROL.—The term ''organizational control'' means the technical and organizational ability to—

(A) allow, deny, or restrict—

(i) an AI agent's access to specific data;

(ii) the actions an AI agent can perform; and

(iii) the tools, information systems, and AI agents which an AI agent can use or interact with; and

(B) revoke or change at any time any of the allowances, denials, or restrictions described in clauses (i) through (iii) of subparagraph (A).