

119TH CONGRESS
2D SESSION

H. R. 10362

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

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 14, 2026

Mr. GOTTHEIMER (for himself and Mr. LAWLER) introduced the following bill; which was referred to the Committee on Science, Space, and Technology, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Stop Rogue AI Act”.

5 **SEC. 2. AI AGENT DISCOVERY AND SECURITY STANDARDS.**

6 (a) AI AGENT DISCOVERY AND SECURITY STAND-
7 ARDS.—

(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;

1 (D) apply discovery and verification con-
2 trols consistently across AI agents regardless of
3 whether such AI agents are developed inter-
4 nally, acquired from third-party vendors, or op-
5 erated through external services;

6 (E) evaluate the security, safety, correct-
7 ness, and reliability of AI agents before such AI
8 agents are deployed by such organization and
9 continuously after such deployment;

10 (F) enable continuous runtime monitoring
11 and, where appropriate, inline detection and
12 interception of AI agent interactions with tools,
13 data sources, information systems, and other AI
14 agents, including detection of prompt injection,
15 data exfiltration, anomalous tool invocation,
16 and behavioral drift from an AI agent's ap-
17 proved operational baseline;

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

22 (H) generate and retain tamper-evident,
23 standardized logs of material AI agent actions,
24 and ensure such logs are portable and acces-
25 sible, as appropriate and consistent with law, to

1 deploying organizations and authorized relying
2 parties.

3 (2) AI AGENT DISCOVERY AS A COMPONENT OF
4 CYBERSECURITY.—In carrying out paragraph (1),
5 the Director, in coordination with the Assistant Sec-
6 retary, shall include in the standards, guidelines,
7 and best practices described in such paragraph AI
8 agent discovery as a necessary component of effec-
9 tive cybersecurity within applicable frameworks, pro-
10 files, and reference materials.

11 (3) OPEN AND INTEROPERABLE DISCOVERY
12 STANDARDS.—The Director, in coordination with the
13 Assistant Secretary, shall support the development
14 and adoption of open, vendor-agnostic, and inter-
15 operable standards for AI agent discovery mecha-
16 nisms. In carrying out this paragraph, the Director
17 and the Assistant Secretary shall—

18 (A) promote the use of existing internet in-
19 frastructure and identity-based discovery mech-
20 anisms, including domain name system-based
21 approaches, cryptographically verifiable AI
22 agent identity and registry frameworks, or func-
23 tionally equivalent mechanisms, to enable secure
24 and scalable AI agent discovery and AI agent
25 identity verification;

1 (B) ensure that such standards are glob-
2 ally interoperable, distributed, and not depend-
3 ent on proprietary or platform-specific reg-
4 istries; and

5 (C) engage with multistakeholder proc-
6 esses, including industry, civil society, and tech-
7 nical standards bodies, to support broad adop-
8 tion and international coordination.

9 (4) MINIMUM ORGANIZATIONAL REQUIRE-
10 MENTS.—Standards, guidelines, and best practices
11 developed under this subsection shall provide that
12 organizations deploying AI agents—

13 (A) maintain a continuous, machine-read-
14 able inventory of all AI agents, using standard-
15 ized, vendor-agnostic naming conventions;

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

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

1 (5) GUIDANCE, COORDINATION, AND DEM-
2 ONSTRATION PROJECTS.—The Director, in coordina-
3 tion with the Assistant Secretary, shall—

4 (A) incorporate the standards, guidelines,
5 and best practices developed under this sub-
6 section into existing National Institute of
7 Standards and Technology frameworks and
8 guidance;

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

15 (C) conduct or support demonstration
16 projects, including through the National Cyber-
17 security Center of Excellence, to evaluate the
18 effectiveness of open agent discovery mecha-
19 nisms;

20 (D) coordinate with the Administrator of
21 the National Telecommunications and Informa-
22 tion Administration to promote outreach and
23 adoption through multistakeholder processes
24 and international engagement, as appropriate;
25 and

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

1 such contract, using standardized, vendor-ag-
2 nostic naming conventions consistent with
3 standards, guidelines, and best practices devel-
4 oped under subsection (a);

5 (B) implement AI agent identity
6 verification mechanisms that are cryptographi-
7 cally verifiable at both the network and applica-
8 tion layers;

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

15 (D) enable the Federal agency that has en-
16 tered into such a contract to exercise organiza-
17 tional control over AI agent activity, including
18 the ability to allow, deny, or constrain AI
19 agent-to-AI agent and AI agent-to-information
20 system interactions;

21 (E) enable the Federal agency that has en-
22 tered into such a contract to provide cryp-
23 tographically verifiable provenance information
24 to authorized entities interacting with the AI

1 agent, consistent with the policies of such Fed-
2 eral agency; and

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

10 (3) REQUIRED CONTRACT ELEMENTS FOR IN-
11 FORMATION SYSTEMS INTERACTING WITH AI
12 AGENTS.—Revisions proposed under paragraph (1)
13 shall ensure contracts for the procurement or de-
14 ployment of information systems that AI agents
15 interact with include requirements that the con-
16 tractor—

17 (A) maintain a continuous, machine-read-
18 able inventory of all AI agents that interact
19 with such an information system, using stand-
20 ardized, vendor-agnostic naming conventions
21 consistent with standards, guidelines, and best
22 practices developed under subsection (a);

23 (B) implement identity verification mecha-
24 nisms that are cryptographically verifiable for

1 all AI agents that interact with such an infor-
2 mation system;

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

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

13 (E) enable the Federal agency that has en-
14 tered into such a contract to exercise organiza-
15 tional control over AI agents' ability to interact
16 with such an information system, including the
17 ability to allow, deny, or constrain AI agent-to-
18 AI agent interactions within such an informa-
19 tion system; and

20 (F) generate tamper-evident, standardized
21 logs of material AI agent actions within such an
22 information system and ensure such logs are
23 portable and accessible to the Federal agency
24 that has entered into such a contract and,

1 where appropriate and consistent with law and
2 such contract, authorized relying parties.

3 (4) SAVING PROVISION FOR CERTAIN CON-
4 TRACTS.—This subsection shall not apply to con-
5 tracts for the procurement or deployment, as the
6 case may be, of AI agents or information systems
7 that interact with AI agents entered into before the
8 date of the enactment of this Act.

9 (5) AGENCY GUIDANCE.—Not later than 180
10 days after the proposal of revisions under paragraph
11 (1) and annually thereafter, the Director of the Of-
12 fice of Management and Budget, in coordination
13 with the Director of the Cybersecurity and Infra-
14 structure Security Agency, shall issue guidance to
15 Federal agencies regarding the following:

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

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

25 (c) DEFINITIONS.—In this section:

1 (1) AI AGENT DISCOVERY.—The term “AI
2 agent discovery” means the technical and organiza-
3 tional capability to identify, enumerate, verify, and
4 maintain a current inventory of AI agents operating
5 within, communicating with, or seeking access to an
6 information system, network, application, service, or
7 digital environment.

8 (2) AI; ARTIFICIAL INTELLIGENCE.—The terms
9 “AI” and “artificial intelligence” have the meaning
10 given the term “artificial intelligence” in section
11 5002 of the National Artificial Intelligence Initiative
12 Act of 2020 (15 U.S.C. 9401).

13 (3) AI MODEL.—The term “AI model” means
14 a software component of an information system that
15 implements artificial intelligence technology and uses
16 computational, statistical, or machine-learning tech-
17 niques to produce outputs from a defined set of in-
18 puts.

19 (4) ARTIFICIAL INTELLIGENCE AGENT; AI
20 AGENT.—The terms “artificial intelligence agent”
21 and “AI agent” mean a software-based system
22 that—

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

1 (B) autonomously interacts with other
2 software systems, digital services, users, exter-
3 nal environments, or AI agents on behalf of a
4 person or organization; and

5 (C) involves minimal or no human inter-
6 action beyond its initial direction.

7 (5) DEFENSE-IN-DEPTH.—The term “defense-
8 in-depth” means the protection of information sys-
9 tems by using multiple security measures, including
10 policies, procedures, and physical security, such as
11 antivirus software, firewalls, anti-spyware tools,
12 strong password policies, intrusion detection sys-
13 tems, biometric verification, encryption, and multi-
14 factor authentication, to reduce the risk of unau-
15 thorized access, data breach, or other successful at-
16 tack.

17 (6) INFORMATION SYSTEM.—The term “infor-
18 mation system” has the meaning given such term in
19 section 3502 of title 44, United States Code.

20 (7) ORGANIZATIONAL CONTROL.—The term
21 “organizational control” means the technical and or-
22 ganizational ability to—

23 (A) allow, deny, or restrict—

24 (i) an AI agent’s access to specific
25 data;

- 1 (ii) the actions an AI agent can per-
2 form; and
- 3 (iii) the tools, information systems,
4 and AI agents which an AI agent can use
5 or interact with; and
- 6 (B) revoke or change at any time any of
7 the allowances, denials, or restrictions described
8 in clauses (i) through (iii) of subparagraph (A).

○