

The Stop Rogue AI Act has a number and a text now. Read the text, not the rollout.

For two weeks this was the House agent-security bill with no public text, only a press release and a preview. Now it is H.R. 10362 and I read it. Here is what it actually requires, what it is not, and one thing the announcement got wrong.

AS OF SEPT 19, 2026: H.R. 10362, “Stop Rogue AI Act,” introduced Sept. 14, 2026 by Rep. Josh Gottheimer (D-NJ-5), with Rep. Mike Lawler (R-NY-17) as original cosponsor. Referred to Science, Space, and Technology, and in addition to Oversight and Government Reform. It is a standards-and-procurement bill, not a ban: NIST standards due within a year of enactment, federal contract rules 18 months after those standards publish. No criminal penalties and no private right of action in the text. The “full text” link on the introducer’s site is a pre-introduction draft with a blank bill number.

1 · WHAT THE BILL ACTUALLY REQUIRES (SEC. 2(A))

NIST, working with NTIA’s Assistant Secretary for Communications and Information, must develop, publish, and maintain standards, guidelines, and best practices for secure agent deployment within one year of enactment, and annually after. The standards must cover, at minimum:

- **Discovery and inventory:** continuously discover, inventory, verify, and keep organizational control over every agent operating within or interacting with the organization’s systems, networks, applications, services, or digital environments — whether built in-house, bought from a vendor, or run through an external service.
- **Runtime monitoring:** continuous monitoring and, where appropriate, inline detection and interception of agent interactions, explicitly including prompt injection, data exfiltration, anomalous tool invocation, and behavioral drift from an approved baseline.
- **Provenance:** cryptographically verifiable mechanisms sufficient to identify the entity responsible for creating or operating an agent.
- **Logs:** tamper-evident, standardized logs of material agent actions, portable and accessible to deploying organizations and authorized relying parties.
- **Control:** the ability to allow, deny, restrict, or revoke an agent’s data access, actions, and the tools and other agents it may touch, at any time.

2 · THE PART WORTH QUOTING: OPEN, VENDOR-AGNOSTIC DISCOVERY

The bill tells NIST to support open, vendor-agnostic, interoperable discovery standards and to promote existing internet infrastructure — “domain name system-based approaches, cryptographically verifiable AI agent identity and registry frameworks, or functionally equivalent mechanisms.” The standards must be globally interoperable, distributed, and explicitly “not dependent on proprietary or platform-specific registries.” Minimum organizational requirements repeat it: a continuous machine-readable inventory using standardized naming, independent cryptographic identity and trust verification at both the network and application layers, and no sole reliance on self-attested or single-provider assertions of identity.

3 · FEDERAL PROCUREMENT IS THE ENFORCEMENT (SEC. 2(B))

The binding part is the buying. Within 18 months after the standards publish, the Federal Acquisition Regulatory Council must propose FAR revisions requiring contractors and agencies that buy or deploy agents (or the systems agents interact with) to comply. Contracts must give the agency an inventory, cryptographic identity and provenance verification, control over agent interactions, and portable logs — and the agency’s discovery and verification must work without relying on the contractor. Contracts entered before enactment are exempt. OMB, with CISA, then has 180 days to issue agency guidance.

4 · THE DEFINITION THAT DOES THE WORK

“AI agent” means 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, external environments, or other AI agents on behalf of a person or organization; and (C) involves minimal or no human interaction beyond its initial direction. That third clause is the whole argument: if a human is watching every step, it is not the thing this bill is about.

WHAT IS NOT PROVEN (READ BEFORE REPEATING)

- **The dates disagree, and the official record wins.** Gottheimer’s own release says the bill was introduced “Wednesday, September 9, 2026.” Lawler’s release page is dated September 15. The GPO text of H.R. 10362 is dated September 14, 2026. Treat Sept. 14 as the introduction date; the release dates are announcement dates.
- **“Full text” is not the introduced text.** The “HERE” link on Lawler’s release points to a PDF dated September 1, 2026 (5:20 p.m.), in legislative-counsel draft form: “H. R. II” with no bill number and a blank committee line. The substance matches the introduced bill, but for a citation use the govinfo version, BILLS-119hr10362ih.
- **It is not a ban.** The title says “rogue.” The mechanism is standards plus procurement. There are no criminal penalties, no fines, no private right of action, and no licensing regime in the text. Compliance reaches the private sector mainly through federal contracts.
- **Nothing here is law, and the timeline is long.** Standards are a year out at the earliest; the FAR rules 18 months after that. Committee action is the next unknown; I found no Senate companion.
- **Cosponsor count:** one, Republican (Lawler), per GovTrack. The bill’s own text lists only Gottheimer as introducer with Lawler joining.

Sources: govinfo.gov, BILLS-119hr10362ih, introduced text, Sept. 14, 2026 (primary) · lawler.house.gov, release + Stop_Rogue_AI_Act_xml.pdf (draft dated Sept. 1, 2026) · gottheimer.house.gov, release dated Sept. 9, 2026 · govtrack.us/congress/bills/119/hr10362 · congress.gov H.R.10362.