COMPETITIVE ENTERPRISE INSTITUTE

1310 L Street NW, 7th Floor • Washington, DC 20005 • www.cei.org

March 9, 2026

Comments of the Competitive Enterprise Institute

RE: Request for Information Regarding Security Considerations for Artificial Intelligence Agents

Docket No.: NIST-2025-0035

The Competitive Enterprise Institute (CEI) appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) Request for Information (RFI) Regarding Security Considerations for Artificial Intelligence Agents. CEI is a non-profit research and advocacy organization that focuses on regulatory policy from a free-market perspective. These comments represent the views of CEI as an organization; they do not purport to represent the views of any individual employee or of any donor.

NIST's RFI rightly recognizes that AI safety and AI security are inextricably linked. By looking beyond traditional cybersecurity concerns, NIST acknowledges that AI security is a spectrum that ranges from conventional software fixes to complex behavioral safeguards. Consequently, NIST should ensure that its safety guidelines are harmonized with enforcement priorities of other federal agencies.

Antitrust Guidelines for Collaborations Among Competitors

Regarding the questions under section 5, "Additional Considerations," it is imperative that NIST prioritize interagency alignment with the Department of Justice (DOJ) and Federal Trade Commission (FTC) in updating guidance that affects collaboration on cybersecurity issues involving AI. This applies most urgently to the application of antitrust law to competitor collaborations and information sharing, where the chilling effect of potential enforcement may discourage collective action to address systemic AI agent vulnerabilities.

On February 23, 2026, the FTC and DOJ launched a joint public inquiry for consideration of new Antitrust Guidelines for Collaboration Among Competitors (Collaboration Guidelines),[1] which

[1] Federal Trade Commission, "Federal Trade Commission and Department of Justice Seek Public Comment for Guidance on Business Collaborations," press release, February 23, 2026, https://www.ftc.gov/news-events/news/press-releases/2026/02/federal-trade-commission-department-justice-seek-public-comment-guidance-business-collaborations; Department of Justice, "Justice Department and Federal Trade Commission Seek Public Comment for Guidance on Business Collaborations," press release, February 23, 2026, https://www.justice.gov/opa/pr/justice-department-and-federal-trade-commission-seek-public-comment-guidance-business.

are due April 24, 2026.[2] Companies have been left "grasping in the dark"[3] since the antitrust agencies withdrew the 2000 Collaboration Guidelines on December 11, 2024,[4] but the DOJ and FTC have a tremendous opportunity to provide clarity for technology companies engaged in the development and deployment of AI systems and infrastructure that power AI agents.

NIST should encourage the FTC and DOJ to consider an antitrust safe harbor for AI safety and security collaborations, because "[f]rontier-model developers would be more likely to collaborate usefully on AI safety and security work if such collaboration were more clearly allowed under the antitrust rules."[5]

2014 Antitrust Policy Statement on Sharing of Cybersecurity Information

NIST should also work with the FTC and DOJ to update their 2014 Antitrust Policy Statement on Sharing of Cybersecurity Information (2014 Policy Statement).[6] The Policy Statement provides a foundational "rule of reason" framework, making clear that sharing technical cyber threat information is generally procompetitive and unlikely to raise antitrust concerns. While the 2014 Policy Statement was wisely omitted from the 2024 withdrawal of the prior Collaboration Guidelines, the NIST RFI regarding AI agent systems introduces novel risks that require an evolution of this policy.

The 2014 Policy Statement requires a more modern definition of "cyber threat information." Presently, the Statement defines threat information primarily through technical indicators like file hashes, malicious URLs, and threat signatures. The definition should be expanded to include AI-specific vulnerabilities identified in the RFI, like indirect prompt injection patterns and adversarial training data/poisoning signatures.

Regulatory Sandboxes

As part of NIST's facilitation of AI safety and security collaboration, the agency should champion regulatory sandboxes to help resolve broader regulatory uncertainty. The Cybersecurity National Lab's 2025 *Regulatory Sandboxes for AI and Cybersecurity* outlines how these environments are critical for addressing the "pace problem" of AI regulation.[7] As Kristian

---

[2] Antitrust Division, Department of Justice, "Collaboration Guidelines RFI Notice," Regulations.gov, February 23, 2026, https://www.regulations.gov/document/ATR-2026-0001-0001.

[3] Dissenting Statement of Commissioner Melissa Holyoak Regarding the Withdrawal of 2000 Antitrust Guidelines for Collaboration Among Competitors, FTC Matter No. V250000, December 11, 2024, p.1, https://www.ftc.gov/system/files/ftc_gov/pdf/holyoak-collaboration-guidelines-withdrawal-statement.pdf.

[4] Federal Trade Commission, FTC and DOJ Withdraw Guidelines for Collaboration Among Competitors," press release, December 11, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-doj-withdrawguidelines-collaboration-among-competitors.

[5] Luke Muehlhauser, "12 Tentative Ideas for US AI Policy," Open Philanthropy, April 17, 2023, https://www.openphilanthropy.org/research/12-tentative-ideas-for-us-ai-policy---/.

[6] Department of Justice and Federal Trade Commission, *Antitrust Policy Statement on Sharing Cybersecurity Information*, April 10, 2014, https://www.ftc.gov/system/files/documents/public_statements/297681/140410ftcdojcyberthreatstmt.pdf.

[7] Filippo Bagni and Fabio Seferi, *Regulatory Sandboxes for AI and Cybersecurity: Questions and Answers for Stakeholders*, February 2025, https://iris.imtlucca.it/bitstream/20.500.11771/34339/1/CybersecNatLab-White-Paper-Regulary-Sandboxes.pdf.

Stout, Director of Innovation Policy at the International Center for Law & Economics, explained in prior comments to the National Telecommunications and Information Administration,

> AI regulators are charged with overseeing a dynamic and rapidly developing market, and should therefore avoid erecting a rigid framework that force new innovations into ill-fitting categories. The "regulatory sandbox" may provide a better model to balance innovation with risk management. By allowing developers to test and refine AI technologies in a controlled environment under regulatory oversight, sandboxes can be used to help identify and address potential issues before wider deployment, all while facilitating dialogue between innovators and regulators. This approach not only accelerates the development of safe and ethical AI solutions, but also builds mutual understanding and trust. Where possible, NTIA should facilitate policy experimentation with regulatory sandboxes in the AI context.[8]

Regulatory sandboxes serve as a "hybrid governance tool" for emerging technologies that can provide a controlled framework to develop, train, validate, and test new products under regulatory supervision.[9] These could provide the types of modified environments for implementing undoes, rollbacks, and negations mentioned in question 4(b) of NIST's RFI.

Respectfully submitted,

Alex R. Reinauer
Research Fellow
Competitive Enterprise Institute
Alex.Reinauer@cei.org

[8] Kristian Stout, Comments of the International Center for Law & Economics, Dual Use Foundation Artificial Intelligence Models with Widely Available Model Weights, Docket No. NTIA-240216-0052, March 27, 2024, https://laweconcenter.org/wp-content/uploads/2024/03/ICLE-NTIA-COMMENTS-RFC-Open-Foundation-Models-2024.pdf.

[9] Filippo Bagni, "Regulatory Sandboxes as a Bridge Between AI and Cybersecurity: Exploring the Interplay Between the AI Act and the Cyber Resilience Act" in Bagni and Seferi, *Regulatory Sandboxes for AI and Cybersecurity*, p. 54.