https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence



<u>Information Technology (https://www.nist.gov/information-technology)</u> /<u>Artificial</u> <u>intelligence (https://www.nist.gov/artificial-intelligence)</u>

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

On July 26, 2024, NIST released four publications intended to help improve the safety, security and trustworthiness of artificial intelligence (AI) systems in support of President Biden's <u>Executive Order (https://gcco2.safelinks.protection.outlook.com/?</u> url=https%3A%2F%2Fwww.whitehouse.gov%2Fbriefing-room%2Fpresidential-

actions%2F2023%2F10%2F30%2Fexecutive-order-on-the-safe-secure-and-trustworthy-developmentand-use-of-artificial-

intelligence%2F&data=05%7C02%7Crachel.trello%40nist.gov%7Cadcb09ad28204cb5dc5c08dcac301a 68%7C2ab5d82fd8fa4797a93e054655c61dec%7C0%7C0%7C638574569852111416%7CUnknown%7CT WFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mno%3D% 7C0%7C%7C%7C&sdata=4nDiZKVtIrn7g8WXvm9%2BuuJh5bUWXsket%2F7FLZm4Nxs%3D&reserve d=0). They include final reports on <u>Generative AI (https://www.nist.gov/artificialintelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence-1), Secure Software</u> (https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificialintelligence/secure), and <u>AI Standards (https://www.nist.gov/artificial-intelligence/executive-order-safe-secure-and-trustworthy-artificial-intelligence/executiveorder-safe-secure-and-trustworthy-artificial-intelligence/ai) and an <u>Initial Public Draft of</u> *Managing Misuse Risk for Dual-Use Foundation Models* (https://www.nist.gov/aisi/guidance). NIST released a draft report on <u>Guidelines for</u> Evaluating Differential Privacy Guarantees (https://csrc.nist.gov/pubs/sp/800/226/ipd) on December 11, 2023.</u>

On November 20, 2024, NIST released a final version of its first synthetic content guidance report on <u>Reducing Risks Posed by Synthetic Content</u> (<u>https://doi.org/10.6028/NIST.AI.100-4</u>).

NIST's Responsibilities Under the October 30, 2023 Executive Order

- <u>NIST's Responsibilities under Executive Order 14110 on Safe, Secure,</u> <u>and Trustworthy AI (https://www.nist.gov/document/nists-responsibilities-under-</u> <u>executive-order-14110-safe-secure-and-trustworthy-ai)</u> (Fact Sheet)
- <u>NIST Announcement on AI Executive Order Actions</u> (<u>https://www.nist.gov/news-events/news/2024/07/department-commerce-announces-new-guidance-tools-270-days-following</u>) (07/26/2024)
- Department of Commerce Announces New Guidance, Tools 270 Days
 Following President Biden's Executive Order on AI
 (https://www.commerce.gov/news/press-releases/2024/07/department-commerce announces-new-guidance-tools-270-days-following) (07/26/2024)
- White House Fact Sheet on AI Actions (https://www.whitehouse.gov/briefingroom/statements-releases/2024/07/26/fact-sheet-biden-harris-administration-announcesnew-ai-actions-and-receives-additional-major-voluntary-commitment-on-ai/) (07/26/2024)
- <u>Department of Commerce Announces New Actions to Implement</u>
 <u>President Biden's Executive Order on AI</u>

(https://www.commerce.gov/news/press-releases/2024/04/department-commerceannounces-new-actions-implement-president-bidens) (04/29/2024)

<u>White House Executive Order Fact Sheet</u>

(https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheetpresident-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/) (10/30/2023)

- Department of Commerce to Undertake Key Responsibilities in Historic AI Executive Order (https://www.commerce.gov/news/pressreleases/2023/10/department-commerce-undertake-key-responsibilities-historic-artificial) (10/30/2023)
- For EO-related questions email: <u>ai-inquiries@nist.gov</u> (<u>https://www.nist.govmailto:ai-inquiries@nist.gov</u>)
- Sign up for AI email alerts <u>here</u> (<u>https://public.govdelivery.com/accounts/USNIST/subscriber/new?topic_id=USNIST_465</u>).

Overview

The <u>President's Executive Order (EO) on Safe, Secure, and Trustworthy Artificial</u> <u>Intelligence (https://www.whitehouse.gov/briefing-room/presidential-</u> <u>actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-</u> <u>artificial-intelligence/)</u> (14110) issued on October 30, 2023, charges multiple agencies – including NIST – with producing guidelines and taking other actions:

- Develop a companion resource to the NIST <u>AI Risk Management Framework</u> (<u>https://www.nist.gov/itl/ai-risk-management-framework</u>), NIST AI 100-1 for generative AI.
- Develop a companion resource to the NIST <u>Secure Software Development</u> <u>Framework (https://csrc.nist.gov/projects/ssdf)</u>to incorporate secure-development practices for generative AI and dual-use foundation models.
- Launch a new initiative to create guidance and benchmarks for evaluating AI capabilities, with a focus on capabilities that could cause harm.
- Develop and help to ensure the availability of testing environments in coordination with the Department of Energy (DoE) and the National Science Foundation (NSF).
- Establish guidelines and processes except for AI used as a component of a national security system to enable developers of generative AI, especially dual-use foundation models, to conduct AI red-teaming tests to enable deployment of safe, secure, and trustworthy systems.
- Initiate an effort to engage with industry and relevant stakeholders to develop guidelines for possible use by synthetic nucleic acid sequence providers.
- Develop a report to the Director of OMB and the Assistant to the President for National Security Affairs identifying existing standards, tools, methods, and practices, as well as the potential development of further science-backed standards and techniques for authenticating, labeling or detecting synthetic content; preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals; and testing software for the above mentioned purposes.
- Create guidelines for agencies to evaluate the efficacy of differential-privacyguarantee protections, including for AI.
- Establish a plan for global engagement on promoting and developing AI standards.

Most of the EO tasks to NIST have a 270 day deadline.

For EO-related questions email: <u>ai-inquiries@nist.gov (https://www.nist.govmailto:ai-inquiries@nist.gov)</u>.



News and Updates



NIST, Nonprofit Research Consortium to Develop Safety Tools for Synthetic Biology to Defend Against Potential Misuse of AI (https://www.nist.gov/news-

<u>events/news/2024/02/nist-nonprofit-research-consortium-develop-safety-tools-</u> <u>synthetic-biology)</u>

February 16, 2024

The cooperative agreement is the next step in NIST's fulfillment of the White House Executive Order on Artificial Intelligence.



<u>U.S. Commerce Secretary Gina Raimondo</u> <u>Announces Key Executive Leadership at U.S. AI</u>

Safety Institute (https://www.nist.gov/news-events/news/2024/02/us-

<u>commerce-secretary-gina-raimondo-announces-key-executive-leadership-us)</u> February 7, 2024

The National Institute for Standards and Technology (NIST) at Commerce will house the U.S. AI Safety Institute.



NIST Offers Draft Guidance on Evaluating a Privacy Protection Technique for the AI Era

(https://www.nist.gov/news-events/news/2023/12/nist-offers-draft-guidance-

evaluating-privacy-protection-technique-ai-era)

December 11, 2023 The agency has made progress on one of its tasks delineated in the rec Order on AI.



<u>NIST Seeks Collaborators for Consortium</u> <u>Supporting Artificial Intelligence Safety</u>

(https://www.nist.gov/news-events/news/2023/11/nist-seeks-collaboratorsconsortium-supporting-artificial-intelligence) November 2, 2023 The AI Safety Institute Consortium will help develop tools to measure and improve AI safety and trustworthiness.

View All News and Updates (https://www.nist.gov/news-events/news-updates/tag/2810041)

Contacts

General Inquiries
 <u>ai-inquiries@nist.gov(https://www.nist.govmailto:ai-inquiries@nist.gov)</u>

Media Inquiries

• NIST Public Affairs Office inquires@nist.gov (https://www.nist.govmailto:inquires@nist.gov)