



New Cybersecurity Guidance Takes Aim at AI-Related Risk

Organizations and individuals have until the end of January to submit feedback on new AI-focused cybersecurity guidance developed by NIST.

In an era where artificial intelligence (AI) is becoming integral to our daily lives, the technology is being put to use on the cybersecurity front. It can analyze vast amounts of data for threat detection, predict potential attacks using behavioral analytics and automate response to security incidents. Unfortunately, these capabilities can also be weaponized by cybercriminals to carry out more sophisticated, damaging attacks.

It's the classic "double-edged sword" technological innovation scenario, and one that the U.S. government is taking seriously. In December, the National Institute of Standards and Technology (NIST) released a preliminary draft of its Cyber AI Profile, which focuses on these three key areas:

- **Securing AI systems:** identifying cybersecurity challenges when integrating AI into organizational ecosystems and infrastructure.
- **Conducting AI-enabled cyber defense:** identifying opportunities to use AI to enhance cybersecurity, and understanding challenges when leveraging AI to support defensive operations.

- **Thwarting AI-enabled cyberattacks:** building resilience to protect against new AI-enabled threats.

What's in the Profile?

Cybersecurity Framework Profile for Artificial Intelligence provides guidelines for using the NIST Cybersecurity Framework to "accelerate the secure adoption of AI," the agency said in a [press release](#). The profile helps organizations think about how to strategically adopt AI while addressing emerging cybersecurity risks that stem from AI's rapid advance. "Regardless of where organizations are on their AI journey, they need cybersecurity strategies that acknowledge the realities of AI's advancement," said NIST's Barbara Cuthill.

The draft resulted from a yearlong effort on the part of NIST cybersecurity and AI experts. Over that time, more than 6,500 individuals contributed to the project. After releasing an initial concept paper in February 2025, conducting a workshop the following April, and hosting a series of community of interest meetings in the summer, NIST released a preliminary draft of the profile for a 45-day public comment period.

Once finalized, the profile will help organizations incorporate AI into their cybersecurity planning by suggesting key actions to prioritize, highlighting special considerations from specific parts of the CSF when considering AI, and providing mappings to other NIST resources, including the AI Risk Management Framework. Cuthill said the authors hope to continue developing the profile as a useful tool.

"The Cyber AI Profile is all about enabling organizations to gain confidence on their AI journey," she said in the press release. "We hope it will help them feel equipped to have conversations about how their cybersecurity environment will change with AI and to augment what they are already doing with their cybersecurity programs."

Helping Organizations Stay Secure

Cybersecurity Dive says NIST's new cybersecurity initiative is part of the agency's broader focus on helping organizations manage AI's benefits and drawbacks. In 2023, the agency released an AI Risk Management Framework, and in 2024 it released a generative AI profile for the framework. In August, NIST published a document intended to help organizations secure their AI systems using the agency's existing and widely adopted security controls catalog.

Through the end of January, NIST is soliciting feedback from the public and will use that input to develop an initial public draft. Following the 45-day comment period, NIST plans to develop the initial public draft for release in 2026.