Holland & Hart

Troy Lyons

Senior Director of Federal Affairs
202.654.6906
Washington, DC
tmlyons@hollandhart.com

What Companies Need to Know: AI Security & Compliance

Insight — June 3, 2026

"nothing in this section shall be construed to authorize the creation of a mandatory governmental licensing, preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models."

With little fanfare, President Donald Trump signed a long-awaited executive order on artificial intelligence (AI) innovation and cybersecurity, following a series of last-minute reversals and internal policy disputes. The order pursues a dual mandate: **accelerating AI innovation** while **strengthening national security against AI-enabled threats**. The signing came after the business community warned administration officials that it was moving too slowly on the issue.

The order's most significant development is its call for technology companies to **voluntarily** submit new AI models to government review prior to public release — a notable shift for an administration that had previously championed a largely hands-off approach to AI regulation.

Notable Provisions

- **30-Day Voluntary Review** — AI companies are asked, but not required, to submit powerful new models for government review 30 days before public release. An earlier draft had proposed a 90-day window, which critics saw as overly burdensome.
- **Cybersecurity Clearinghouse** — The Treasury Department has 30 days to establish a clearinghouse in partnership with AI developers and critical infrastructure owners to identify and address vulnerabilities.
- **Classified Benchmarking Process** — An National Security Agency (NSA) led initiative to assess the national security implications of advanced AI models.
- **Pentagon Network Security** — A 30-day deadline to secure military networks against AI-enabled threats.
- **DOJ Criminal Enforcement** — Directs the Attorney General and Department of Justice to prioritize the prosecution of individuals who use AI to violate cybercrime, identity theft, and fraud laws.
- **Expanded Access for State, Local, and Critical Infrastructure Entities** — Advises the Cybersecurity and Infrastructure Security Agency to facilitate access to AI-capable cybersecurity tools for state and local governments and critical infrastructure operators, including rural hospitals, community banks, and local utilities. The

order also directs expedited civilian federal cybersecurity efforts and expanded AI-enabled defensive capabilities.

Bottom Line

This executive order represents the most significant step yet by the federal government towards regulating AI. It attempts to strike a balance between the administration's pro-innovation, anti-regulation posture and growing national security concerns about AI's potential to expose and exploit critical cybersecurity vulnerabilities. Predictably, critics on both sides question whether it goes too far or not nearly far enough.

This tension is unlikely to be resolved anytime soon. AI governance will remain a flashpoint across multiple fronts — from federal policy and data center development (where community opposition and congressional scrutiny are intensifying) to the broader questions around how to deploy these technologies at scale responsibly.

Congressional attention to AI is accelerating, specifically in lawmakers beginning to examine legislation addressing AI's potential workforce disruptions, copyright protections, energy uses, and small business impact. A central point of contention is whether federal law should preempt the rapidly expanding patchwork of state-level AI regulations. As with any executive action, the real-world impact of this order will ultimately be determined by how it is implemented — and by the degree of voluntary cooperation from the technology industry.

For more details on the Executive Order, read this article.
