Matt Shell

Associate
775.327.3000
Reno
smshell@hollandhart.com

IP, Privacy, and Criminal Liability: The AI Executive Order's Private-Sector Impact

Insight — June 3, 2026

On June 2, 2026, President Trump signed an executive order titled, “Promoting Advanced Artificial Intelligence Innovation and Security” (EO) addressing AI and national cybersecurity. While directed primarily at federal agencies, the order carries significant information security and data privacy implications for private-sector companies—particularly AI developers, critical infrastructure operators, and enterprises that handle sensitive data.

Key elements include a new AI cybersecurity clearinghouse with voluntary private-sector participation, a framework for pre-release government access to frontier AI models, expanded AI-enabled cybersecurity tools for critical infrastructure, and heightened criminal enforcement against AI-enabled intrusions. The EO expressly disclaims any intent to create mandatory licensing or preclearance requirements for AI model development or release.

The EO takes an “America First” approach to AI—favoring innovation and voluntary government-industry partnership over heavy-handed regulation. Unlike some state laws that impose specific AI requirements, the federal order steers clear of mandatory licensing or approval processes. Instead, it invites companies to work with agencies on cybersecurity, while protecting their proprietary technology. The bottom line for businesses: the federal government is paying closer attention to AI security risks, and companies—particularly those handling sensitive data or operating in critical sectors—should weigh whether participating in voluntary federal programs makes sense for them.

Key Takeaways

AI Developers. Assess the IP and data privacy risks of the voluntary frontier model framework, including government NDA adequacy and FOIA exposure. Monitor the classified benchmarking process.

Critical Infrastructure Operators. Evaluate how new AI-enabled cybersecurity tools interact with existing regulatory obligations (HIPAA, GLBA, state breach notification laws) and vendor management frameworks.

Clearinghouse Participants. Negotiate clear terms on confidentiality, use, and retention of shared vulnerability data before engaging with the clearinghouse.

Companies Deploying AI Agents. Review access governance and oversight controls to ensure AI agent activities remain within authorized parameters and reduce CFAA exposure.

1. Information Security Implications (Section 2)

The EO directs the Secretary of the Treasury, in consultation with the National Cyber Director, the Secretary of War (through the Director of the National Security Agency), and the Secretary of Homeland Security (through the Director of CISA), to form an AI cybersecurity clearinghouse within 30 days that will operate in voluntary collaboration with the AI industry and critical infrastructure operators to coordinate vulnerability scanning, discovery, validation, and patch distribution. Companies that participate should consider the confidentiality implications of sharing vulnerability data with the government, including the handling of proprietary security findings and the risk that disclosed vulnerabilities could be exploited before remediation.

Separately, the Cybersecurity and Infrastructure Security Agency (CISA) must release Binding Operational Directives within 30 days to facilitate access to AI-enabled cybersecurity tools for agencies, state and local authorities, and critical infrastructure operators (including rural hospitals, community banks, and local utilities). Organizations in these sectors should evaluate how AI-enabled defensive tools interact with existing data protection obligations (e.g., HIPAA, GLBA) and vendor management frameworks.

2. Data Privacy and Intellectual Property Implications (Section 3)

Within 60 days, the Secretary of the Treasury, the Secretary of War (through the Director of NSA), and the Secretary of Homeland Security (through the Director of CISA)—in consultation with the White House Chief of Staff (through the National Cyber Director), the Assistant to the President for Science and Technology, and the Secretary of Commerce (through the Director of NIST)—must design a voluntary framework under which AI developers may provide the federal government with access to "covered frontier models" up to 30 days before release to trusted partners, subject to "appropriate confidentiality, cybersecurity, insider-risk, and intellectual-property protection, use, and nondisclosure requirements." Developers considering participation should assess the trade secret and data privacy risks of pre-release government access—including FOIA exposure, the scope of government use rights, and the potential for reverse engineering or independent development claims.

Agencies must also establish a classified benchmarking process (with the NSA Director making the final determination) to designate which models qualify as "covered frontier models." Because the criteria will be classified, developers may face uncertainty about whether their models trigger the designation until they voluntarily submit to the process.

The EO explicitly provides that nothing in Section 3 authorizes mandatory licensing, preclearance, or permitting for the development or distribution of AI models. Companies should nonetheless monitor whether the voluntary

framework creates de facto market pressures over time.

3. Criminal Enforcement and AI Agent Liability (Section 4)

The Attorney General must prioritize enforcement of the CFAA (18 U.S.C. § 1030), wire fraud, identification document fraud, and other federal criminal statutes against anyone who uses AI—including AI agents—to illegally access or damage computers or to further any other crime. Companies deploying autonomous AI agents should review access governance frameworks, logging, and human oversight controls to mitigate the risk that automated AI activities could be characterized as unauthorized access under the CFAA.

Because the EO's implications will vary depending on a company's industry, data practices, and level of engagement with federal cybersecurity programs, companies should consult with experienced privacy and data security counsel to assess how these developments apply to their specific operations and to develop a tailored compliance strategy as the EO's implementing directives take shape.

For a Federal Affairs perspective on the Executive Order, read here.
