Artificial Intelligence Update

June 2026

AI Meets National Security—Implications for Private Equity and M&A

Key Notes:

- The White House issued the executive order "Promoting Advanced Artificial Intelligence Innovation and Security," advancing AI innovation while strengthening cybersecurity and national security protections for advanced and frontier AI systems.
- The order directs agencies to prioritize cyber defense of government and critical infrastructure, create an AI cybersecurity clearinghouse, develop a classified benchmarking process for "covered frontier models," and establish a voluntary framework for developer engagement on model classification and early access.
- This is especially important for M&A and private equity because AI is now a core diligence and governance issue, requiring heightened scrutiny of model security, data provenance, AI-agent controls, and readiness for emerging federal frameworks in software, data-intensive, regulated, and critical-infrastructure transactions.

On June 2, 2026, President Trump signed the executive order "Promoting Advanced Artificial Intelligence Innovation and Security," a policy move that reaffirms the United States' commitment to leading the global AI race while also tightening the focus on cybersecurity and national security risks associated with advanced AI systems. The order sends a clear signal to the private sector: AI is no longer just a competitive differentiator or a technology trend—it is a strategic national priority with material implications for how companies develop, deploy, and govern AI. For private equity sponsors, strategic acquirers, and their portfolio companies, this means AI is moving from the periphery of diligence and governance discussions into the center of transaction planning, risk management, and post-closing integration.

The executive order balances two seemingly competing objectives: accelerating AI innovation and strengthening security. On the innovation side, the administration emphasizes reducing unnecessary regulatory friction, expanding federal support for AI research and development, and encouraging public-private partnerships. The order also makes clear that the federal government will not impose mandatory licensing, preclearance, or permitting regimes on the development or release of AI models. On the security side, however, the order directs federal agencies to take concrete steps to protect government and critical infrastructure systems from AI-enabled cyber threats, to establish a classified benchmarking process for advanced AI models, and to create a voluntary framework for collaboration with developers of "covered frontier models." This dual-track approach reflects a policy reality that will shape deal dynamics in the years ahead: innovation will be encouraged, but security and compliance will be non-negotiable.

The order sets in motion a series of agency actions with tight timelines. Within 30 days, the Committee on National Security Systems and the Department of War must prioritize cyber defense of National Security Systems and Department of War information systems, respectively. The Department of Homeland Security, acting through CISA and in consultation with OMB and the National Cyber Director, must issue Binding Operational Directives to expedite cyber defense of civilian federal systems, expand AI-enabled

cybersecurity services, and facilitate access to cybersecurity tools, including covered frontier models, for federal agencies, state and local authorities, and critical infrastructure operators such as rural hospitals, community banks, and local utilities. The order also directs the Department of the Treasury, in consultation with NSA, CISA, and others, to establish an AI cybersecurity clearinghouse to coordinate vulnerability scanning, validate software vulnerabilities, and coordinate remediation and patch distribution.

Within 60 days, OMB must assess whether existing federal grant programs can fund advanced AI vulnerability detection efforts, and the Office of Personnel Management must expand the United States Tech Force Information Cybersecurity Specialist hiring pathways to address the federal cybersecurity workforce gap. The Department of the Treasury, through NSA and CISA and in coordination with NIST, must develop a classified benchmarking process to assess the advanced cyber capabilities of AI models and determine the threshold for designation as a "covered frontier model." The order also establishes a voluntary framework under which AI developers can engage the federal government to determine whether a model qualifies as a covered frontier model, provide early access to the government up to 30 days before broader release, and collaborate in selecting trusted partners for early access. All of these activities are subject to confidentiality, cybersecurity, insider risk, IP protection, and nondisclosure requirements.

The order also directs the Attorney General to prioritize enforcement of existing criminal statutes, including 18 U.S.C. §§ 1028, 1030, and 1343, against actors who use AI to illegally access or damage computers, breach IT systems, or employ AI agents to unlawfully access data for criminal or unlawful purposes. This enforcement priority elevates the stakes for companies that deploy AI tools or agents without adequate controls, training, and oversight. Weak AI governance can now be framed not only as a compliance or reputational risk, but also as a potential source of criminal and civil exposure for both individuals and organizations.

For private equity sponsors and M&A buyers, the order has immediate and practical implications. Transactions involving AI developers, software companies, data-intensive platforms, cybersecurity providers, critical infrastructure vendors, and any business that relies on advanced AI models should now expect more focused diligence on model governance, data architecture, security controls, and regulatory exposure. Buyers should assess whether a target's models could meet future "covered frontier model" thresholds, based on factors such as compute capacity, deployment scale, integration with federal or critical infrastructure systems, and intended use cases. Even if a model does not currently qualify, the order sets in motion a classified benchmarking process that may reclassify systems as they evolve. This means diligence must account for both current and potential future regulatory categorization.

Data architecture and model training practices are now central to AI-related risk. Buyers should evaluate data provenance, licensing, and chain-of-custody for training data; whether data is properly segmented between customers, models, and internal use; and whether models are trained on public, proprietary, or third-party data with restrictive terms. These issues directly expose sellers and buyers to IP, trade secret, and unfair competition claims, and they are likely to be scrutinized in both regulatory and commercial diligence.

The order's emphasis on an AI cybersecurity clearinghouse and federal vulnerability scanning also suggests heightened expectations in several areas: proactive vulnerability detection and remediation, documented patch management processes, penetration testing and red-teaming (especially for AI-enabled systems), and incident response plans that specifically address AI agents, model abuse, and prompt injection-style attacks. Transactions should evaluate whether the target's cybersecurity program would satisfy diligence expectations from regulated customers, government contractors, or federal partners.

The order's focus on AI agents used to unlawfully access data means buyers should carefully review agent architecture and permissions, identity and access management for AI agents, logging, monitoring, and audit trails for agent actions, and controls against unauthorized automation that could blur into "unauthorized access" under criminal statutes.

In light of these developments, buyers may consider more specific AI-related representations on model governance,

data provenance, security controls, and third-party dependencies; covenants requiring maintenance of AI security policies and incident response plans; and indemnities covering AI-related IP, data, and cybersecurity claims. For sellers interested in federal collaboration under the voluntary frontier model framework, diligence should assess readiness to engage with NSA, CISA, and NIST on model classification; the ability to support early access under confidentiality and security requirements; and whether the seller's IP and confidentiality controls are adequate for trusted-partner agreements.

From a governance perspective, boards and management teams should treat AI as a core enterprise risk, not just a technology issue. AI-related controls, policies, and oversight mechanisms should be integrated into the broader risk management framework, with clear accountability at the board and executive level. Companies should consider updating AI ethics and acceptable use policies, strengthening training and oversight for staff using AI tools or agents, and improving incident documentation and reporting practices. For portfolio companies in regulated sectors or those with government-adjacent business, these considerations are especially important, as emerging federal expectations are likely to be reflected in customer diligence, procurement requirements, and regulatory inquiries.

The practical takeaway for PE sponsors and M&A leaders is straightforward: AI is now a transaction issue, a governance issue, and a cybersecurity issue at the same time. Buyers should build AI-specific diligence into their processes now, rather than waiting for those issues to surface in customer negotiations, regulator inquiries, or post-closing integration. Action items include updating AI diligence checklists to include model classification risk, data provenance, agent security, and readiness for federal vulnerability frameworks; requiring technical due diligence workstreams focused on AI architecture, security controls, and AI-specific incident response; developing post-closing integration plans that address AI governance, security tooling, and vulnerability management; and evaluating whether AI-related controls meet emerging federal expectations for portfolio companies in regulated sectors.

The executive order is a clear signal that the federal government views AI as central to U.S. economic and national security strategy. For private equity and M&A professionals, the best path forward is to treat AI as a core component of deal strategy, diligence, and portfolio value creation, rather than as a peripheral technical detail. Companies that proactively address AI governance, security, and compliance will be better positioned to navigate the evolving regulatory landscape, meet customer and investor expectations, and unlock value in both transactional and operational contexts.

FOR MORE INFORMATION

For more information, please contact:

Will M. Henry
216.566.7077
William.Henry@ThompsonHine.com

Sachin Java
216.566.5637
Sachin.Java@ThompsonHine.com