Peckar & Abramson, P.C. | ALERT

PRESIDENTIAL ACTION ALERT

Richard R. Volack
rvolack@pecklaw.com

Denis Serkin
dserkin@pecklaw.com

New Executive Order on AI Innovation and Security: Key Takeaways for the Construction Industry

On June 2, 2026, President Trump signed an Executive Order titled "Promoting Advanced Artificial Intelligence Innovation and Security." At its core, the Order is a cybersecurity and national-security measure rather than a broad regulation of how private companies develop or use AI. It directs federal agencies to harden government systems against AI-enabled cyber threats, establishes voluntary frameworks for collaboration between the federal government and the AI and critical-infrastructure sectors, and strengthens criminal enforcement against the malicious use of AI.

Notably, the Order expressly disclaims any intent to create a "mandatory governmental licensing, preclearance, or permitting" regime for the "development, publication, release, or distribution of new AI models." Instead, the Executive Order seeks to "promote AI innovation and security" by working with the private sector to modernize government and private-sector information systems and harden them against external threats, protect intellectual property from exploitation or theft, and cultivate American AI capabilities.

Although the Order does not directly target the construction industry, several provisions are relevant to construction, engineering, and infrastructure firms, particularly those working on energy, utility, power-generation, and other critical infrastructure projects, as well as those holding federal government contracts. We summarize the key provisions and their practical implications below.

Key Directives from the Executive Order

- **Hardening federal and national-security systems.** Within 30 days, agencies, including the Department of War, Cybersecurity and Infrastructure Security Agency ("CISA"), and the Committee on National Security Systems are directed to prioritize the cyber defense of national security systems, Department of War information systems, and civilian federal government information systems, and CISA is to issue "Binding Operational Directives" and related guidance and tools.

- **AI Cybersecurity Clearinghouse.** The Treasury Department, in collaboration with the National Security Agency ("NSA") and CISA, will establish an AI cybersecurity clearinghouse in voluntary collaboration with the AI industry and critical-infrastructure operators to coordinate vulnerability scanning, validation, and the prioritization and distribution of security patches and remediation. The Order also directs the OMB to determine whether there are grant programs available so that relevant funding can be directed to applications that are developing these security measures.

- **Broader access to AI cyber tools.** CISA will facilitate access to cybersecurity tools and services, including certain "covered frontier models," for agencies, state and local authorities, and operators of critical infrastructure, such as local utilities, community banks, and rural hospitals.

- **Secure frontier-model framework.** The government will establish a classified benchmarking process to "assess the advanced cyber capabilities of AI models," determine which models should be designated as a "covered frontier model," and establish a voluntary framework for early access by the government and "trusted partners." Participation is voluntary, and no governmental license or permit is required to develop or release new AI models.
- **Criminal enforcement priority.** The Attorney General is directed to prioritize enforcement of federal computer-fraud, wire-fraud, and identity-fraud statutes against those who use AI, including autonomous "AI agents," to unlawfully access "data or information that is subsequently used for a criminal or unlawful purpose."

Why It Matters for Construction and Infrastructure Firms

- **Energy, utility, and critical-infrastructure work is the most directly affected.** Contractors, EPC firms, and design professionals who build, service, or operate critical infrastructure, power generation and transmission, renewables, water, and other utility assets fall within the universe of "critical-infrastructure operators" that the Order targets for voluntary collaboration and access to tools. Because these projects increasingly integrate networked operational technology such as supervisory control and data acquisition systems ("SCADA"), building management systems ("BMS"), smart-metering, and connected jobsite equipment, the cybersecurity expectations the Order signals will extend to design specifications, commissioning, and as-built deliverables, not just the office or construction trailer IT environment. These firms should watch for opportunities to engage with the clearinghouse and benefit from enhanced federal cyber resources, while anticipating heightened cybersecurity expectations baked into project requirements from procurement through closeout.
- **Federal contractors should anticipate cybersecurity flow-down.** CISA's forthcoming "Binding Operational Directives" apply directly to federal agencies, but in practice, these requirements often appear in procurement and prime/subcontract terms. Construction firms with federal work, including civil and military projects, should monitor new or tightened cybersecurity obligations for their internal and project IT systems that may be reflected in solicitations and contract clauses, and, in turn, flow-down these obligations to subcontractors, suppliers, vendors, and design consultants. Primes should review their subcontract and purchase-order forms now so that any new directives can be flowed down the chain without leaving gaps in coverage or indemnity.
- **Cyber-fraud exposure remains acute.** Construction is a frequent target of payment diversion and business email compromise schemes—often built around spoofed payment applications, fraudulent lien-waiver or change-order requests, and last-minute bank-instruction changes during a draw cycle, which are now increasingly AI-enabled and harder to detect. The Order's enforcement priority and the new clearinghouse resources are positive developments, but firms should reassess wire-transfer controls, subcontractor and vendor banking-detail verification (including callback protocols), heightened IT system security protocols, and incident-response plans in light of more sophisticated, AI-driven threats.
- **AI adoption proceeds under a light-touch federal posture, with guardrails.** The Order signals continued federal support for rapid AI adoption and no new licensing burden for developers or users. Firms deploying

AI tools (including agentic systems) for estimating, scheduling, BIM and design coordination, document review, and project administration retain broad latitude but should ensure that governance, system security, and access controls are heightened or at least keep pace with industry standards, given the Order's focus on the criminal misuse of AI agents. Particular care is warranted when agentic tools can act on a firm's behalf, initiating payments, issuing purchase orders, or transmitting bid and pricing data, so that authentication, authorization limits, and audit logging align with the autonomy granted.

Recommended Next Steps

- Monitor the forthcoming CISA "Binding Operational Directives," the Treasury-led clearinghouse framework, and the frontier-model benchmarking process as implementation details emerge over the next 30–60 days.
- Review internal cybersecurity and AI-governance policies, audit cybersecurity representations, flow-down provisions, and incident-notification requirements across RFPs, bid proposals, prime contracts, subcontracts, purchase orders, design-consultant agreements, and IT-vendor agreements, and confirm that obligations accepted upstream can be passed through downstream for existing and pending federal and critical-infrastructure projects.
- Tighten payment-fraud controls now, mandate callback or human verification for any change to subcontractor or vendor banking instructions, require dual approval for wire transfers and pay-application disbursements, and refresh training for accounting and project teams on AI-enabled spoofing, phishing, or social engineering.
- For energy, utility, and infrastructure clients, evaluate whether to participate in voluntary federal programs and how enhanced tool access can be leveraged for current and upcoming projects.