GOODWIN

ALERT · JULY 1, 2025

The Devil's in the Details: Executive Order on Cybersecurity Reveals Administration's Focus on AI-Cyber Convergence, Secure Software Development, and Foreign Threats

BY Kaitlin Betancourt Peter M. Marta L. Judson Welle Liza Craig Corey Berman

On June 6, 2025, President Trump issued an Executive Order entitled "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144" (the "Order"). The measure sets forth revised cybersecurity priorities for the administration and modifies certain Biden- and Obama-era cybersecurity programs and initiatives. The Order, along with the accompanying White House Fact Sheet, focuses primarily on federal government agencies and provides insight into the administration's developing policy preferences as the president "reprioritizes" U.S. cybersecurity policy.

The Order rescinds or amends portions of Executive Order 14144, which President Biden issued during his final days in office and which we addressed here. The Order's amendments largely remove prescriptive elements from that prior measure, some of which are addressed elsewhere in Office of Management and Budget ("OMB") directives and National Institute of Standards and Technology ("NIST") guidance. The Order is less a seismic shift in policy than a set of adjustments in governance tactics and a reduction in compliance requirements for federal agencies.

The Order, together with President Trump's earlier Executive Order ("the AI EO") revoking the Biden administration's landmark directive on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," underscores the administration's intent to establish a distinct governing philosophy on cybersecurity regulation and artificial intelligence ("AI") governance and highlights the increasing convergence of AI and cybersecurity.

AI and Cybersecurity

The Order addresses the critical intersection of AI and cybersecurity with its emphasis on secure software. While acknowledging that AI "has the potential to transform cyber defense by rapidly identifying vulnerabilities, increasing the scale of threat detection techniques, and automating cyber defense," the Order rescinds certain specific AI initiatives and pilot programs, but retains many security provisions related to AI. It preserves the directive for the Secretaries of Defense and Homeland Security, along with the Director of National Intelligence, to integrate AI software vulnerability management into existing vulnerability assessments, incident response, and information-sharing programs. AI software vulnerability management is arguably one of the more critical and imminent risk areas at the intersection of cybersecurity and AI. The Order also directs an interagency effort to make cyber defense research data available to the academic research community "in consideration of business confidentiality

and national security."

The Order eliminates a directive for a public – private pilot program involving the Departments of Energy, Defense, and Homeland Security to explore uses of AI in securing critical energy infrastructure. The rescinded program was intended to support vulnerability detection, automatic patch management, and the identification of anomalous cyber activity. The Order also revokes the directive for the Secretary of Defense to establish a cyber defense program utilizing advanced AI tools, and it reverses plans for a formalized interagency research agenda focused on human – AI interaction methods for defensive cybersecurity, AI-generated code security, secure AI system design, and cyber incident response pertaining to AI systems.

Certain proactive cyber defense initiatives may be revived elsewhere, such as via the AI "action plan" the administration ordered to be promulgated in the AI EO. In that action, President Trump directed the Executive Office of the President to work toward the goal "to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." On April 24, as part of the AI action plan's development, the White House Office of Science and Technology Policy published more than 10,000 public comments stemming from a formal Request for Information. It is possible that the forthcoming plan, expected by the end of July, will include additional initiatives and investments and may replace some of the Biden-era programs rescinded by the Order.

The latest adjustments largely reflect the broader Trump administration effort to prioritize development as part of a strategy to position the U.S. as a global leader in AI innovation, which we discussed here. The Fact Sheet notes that the Order "refocuses [AI] cybersecurity efforts towards identifying and managing vulnerabilities, rather than censorship." Proactive uses of AI, even in cyber defense, may be addressed by the administration separately, as part of the AI action plan, for example.

In April of this year, as part of the implementation of the AI EO, OMB issued two AI-focused memoranda that will be implemented in the months ahead. These memoranda aimed to strengthen federal government AI policy by directing AI governance and responsible deployment across agencies and encouraging AI risk management in federal procurement policy.[1] The memoranda encourage procurement of American-made AI products and services and impose detailed requirements for agencies throughout the lifecycle of AI acquisition – from identifying high-impact AI uses to conducting appropriate market research, avoiding vendor lock-in, and overseeing contract performance. While the AI EO itself was high-level, the OMB memoranda, which stemmed from the AI EO's directive to OMB to issue guidance, are quite prescriptive and comprehensive.

Software Development Security and Federal Procurement

The Order retains an emphasis on software supply chain cybersecurity. It retains much of the Biden administration's framework but scales back prescriptive directives and enforcement mechanisms, particularly those related to secure software development "attestations."

Under President Biden's plan, the Cybersecurity and Infrastructure Security Agency ("CISA") was tasked with developing a program to verify software provider security attestations and report to the National Cyber Director, who would in turn publicly disclose attestation validation results and refer entities that failed validation to the Attorney General for potential enforcement action. The Order eliminates this directive.

Elsewhere, the Order maintains efforts to promote secure software development through public – private engagement. It maintains a plan to organize an industry-facing consortium housed at the National Cybersecurity Center of Excellence, in consultation with NIST, with the aim of issuing guidance implementing NIST's Special Publication 800-218 (Secure Software Development Framework). The Order instructs NIST to update Special Publication 800-53[2] (Security and Privacy Controls for Information Systems and Organizations), which establishes controls for systems and organizations and is mandatory for federal information systems in accordance with OMB Circular A-130. NIST Special Publication 800-218 already contains prescriptive controls and provides that it is important for organizations to consider the evidence (artifacts, documentation) that will be needed to support current and future control assessments.

Further, the Order retains the directive to the OMB to issue guidance, including any necessary revision to Circular A-130.

Circular A-130 imposes information security and privacy requirements with which federal agencies must comply when managing information resources, limiting the effect of the Order's removal of President Biden's requirement for NIST to identify "minimum cybersecurity practices" for hardening networks against threat actor compromise. Circular A-130 places ultimate responsibility for compliance with its requirements upon agencies, which in turn must describe responsibilities of service providers in relevant agreements with such service providers.

Through OMB memoranda and NIST mandatory guidance, several strict requirements are retained under the current administration, although they are no longer front and center in the Order itself. With respect to procurement, prescriptive requirements apply via Circular A-130, which requires federal agencies to take ultimate responsibility and flow down requirements to service providers. Of course, and not surprisingly, the de-emphasis on enforcement is a noteworthy policy shift but several requirements on secure software development and procurement are largely retained.

In line with the emphasis on secure software procurement, the Order recognizes that federal information security "relies on the security of the Government's cloud services" and retains an interagency plan to develop FedRAMP policies to incentivize — or in some cases require — cloud service providers to assist agencies in configuring cloud-based systems to secure federal agency data.

National Security

Focus on Foreign Cyber Threats: The Order narrows President Obama's Executive Order 13694 by limiting cybersecurity-related sanctions designation authority to apply to only *foreign* persons. The sanctions designation is designed to address malicious cyber activity threatening U.S. national security, foreign policy, economic health, or financial stability via activities such as compromising U.S. networks, misappropriating trade secrets, undermining elections, or engaging in ransomware attacks. The narrowing of the sanctions designation authority suggests the administration's particular enforcement scrutiny centered on malicious foreign actors.

This amendment aligns with the continued federal government focus on nation-state cyber actors and threats. Of note, on July 8, 2025, the Department of Justice will begin enforcing a sweeping rule restricting access to Americans' bulk sensitive personal data by "countries of concern," including China, Russia, Iran, and North Korea — nations explicitly identified as significant cyber threats in the Order's revised policy statement.

Space System Cybersecurity: The Order maintains the Biden-era emphasis on cybersecurity threats to space systems. Agencies are directed to verify that federal space systems incorporate cybersecurity best practices, including "continuous assessments, testing, exercises, and modeling and simulation." In addition, the Departments of the Interior and Commerce, along with NASA, are instructed to review and recommend updates to civil space contract cybersecurity requirements.

Other Notable Provisions

Cyber Trust Mark for IoT Devices: The Order continues support for amendments to the Federal Acquisition Regulation ("FAR") limiting procurement of consumer Internet of Things ("IoT") products to vendors that carry the Federal Communications Commission's voluntary " Cyber Trust Mark" by January 2027. The cybersecurity label is designed to help consumers make informed purchasing decisions and to incentivize manufacturers to adopt stronger cybersecurity controls. Eventually, if an IoT product does not carry this mark, it will be excluded, per the FAR and agency-specific regulations, from the federal procurement process entirely.

Rescission of Digital Identity Verification: The Order rescinds the prior policy encouraging the use of digital identity credentials for accessing public benefit programs. The Biden administration had directed the development of digital identity documentation, and, to reduce fraudulent transactions, notifications to individuals when their identity data was used to request public benefit payments. The Trump administration's Fact Sheet states that digital identification efforts are

outside the Order's "core cybersecurity focus." Digital identity verification practices may continue to develop at the state level, but federal-level support is unlikely to continue in the near future.

Takeaways

1. **AI and Cyber Are Inextricably Intertwined**. Companies should view the Order as an adjustment to the administration's governance preferences and enforcement focus, rather than a major pivot. While specific White House support for individual pilot programs has been rescinded, other initiatives are underway that may supplant these initiatives, such as a recently announced Department of Defense contract with OpenAI to develop frontier AI capabilities for national security. Companies should closely track the administration's forthcoming AI Action Plan, and take a cue from the OMB memoranda on AI governance and procurement, which provide that AI governance is key to accelerated innovation. Companies should further take note of the administration's emphasis on AI software vulnerability management as a key cybersecurity concern and recognize the increasing importance of AI security.
2. **Secure Software Remains a Priority**. Although the Order rolls back certain enforcement tools related to federal agency procurement efforts, technology vendors and software providers may find that mandatory requirements and controls remain and that market expectations continue to favor adherence to prior frameworks. Moreover, forthcoming NIST guidance and possible future OMB or other memoranda may reintroduce some structured requirements from earlier presidential directives. Impacted entities should monitor evolving secure software guidance — particularly updates to NIST Special Publications 800-218 and 800-53 — and track the progress of other initiatives such as the rollout of the Cyber Trust Mark. Developers and consumers of software products and cloud services should be mindful of the continued emphasis on secure software development through updated standards and industry collaboration, and they should proactively align their cybersecurity controls and programs with NIST's evolving best practices.
3. **Foreign Cyber Threats**. The Order sharpens the administration's cybersecurity posture with a clear emphasis on threats posed by foreign actors, and names specific countries of concern. From the revised policy statement identifying specific nations as cyber threats to the narrowing of earlier sanctions designation authority, the Order and accompanying Fact Sheet demonstrate a continued view of cybersecurity as a major national security concern. Combined with the rollout of the Department of Justice's restrictions on sharing bulk sensitive data, the Order signals that companies with exposure to foreign markets, in particular those handling sensitive data or critical infrastructure, should expect continued enforcement and scrutiny.

---

[1] Memo M-25-21 ("Accelerating Federal Use of AI through Innovation, Governance, and Public Trust") directs federal government agency AI governance, transparency, and responsible deployment. Memo M-25-22 ("Driving Efficient Acquisition of Artificial Intelligence in Government") encourages federal government AI procurement and risk management.

[2] NIST Special Publication 800-53, mandatory for federal information systems, is 492 pages long and established due diligence controls in managing information security and privacy risk, including by establishing a comprehensive risk management program.

CONTACTS

Kaitlin Betancourt
Partner

kbetancourt@goodwinlaw.com
New York | +1 212 813 8936

Peter M. Marta
Partner

petermarta@goodwinlaw.com
New York | +1 212 813 8048

L. Judson Welle
Partner

jwelle@goodwinlaw.com
New York | +1 212 459 7400

Liza Craig
Partner

lcraig@goodwinlaw.com
Washington, DC | +1 202 346 4171

Corey Berman
Associate

coreyberman@goodwinlaw.com
New York | +1 917 229 7503