POLSINELLI

# Publications

July 7, 2025 • Publications

## A New Executive Order Signals Administration's Cybersecurity Priorities

### Key Takeaways

- President Trump's new cybersecurity Executive Order largely retains the structure and goals of EO 14144 but rolls back several deadlines and prescriptive directives to give agencies more flexibility.
- The new Executive Order will affect a wider private industry audience, which can anticipate new federal initiatives focused on strengthening software supply chains, improving cloud security and integrating AI into cybersecurity efforts.
- While the new Executive Order maintains core cybersecurity priorities, such as software supply chain security, enhanced Federal Risk and Authorization Management Program (FedRAMP) requirements and encryption of federal communications, it scales back or eliminates mandates like software attestation, digital identity directives and funding for AI pilot programs, shifting toward guidance and agency discretion.
- The Executive Order sustains long-term initiatives like the Cyber Trust Mark labeling program and narrows sanction authority for malicious cyber activity to foreign individuals only, signaling continued federal cybersecurity enforcement with a more targeted and flexible approach.

On June 6, 2025, President Trump signed a new Executive Order, titled "Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144" (Executive Order).This recent Executive Order enumerates a number of key cybersecurity issues that we can expect to see increased focus on from the federal government in the near term. At a high-level, the Executive Order is framed to "strengthen the nation's cybersecurity," and government contractors will likely be the first ones to react and adjust to the new requirements. However, as discussed below, several of the new Executive Order's initiatives will likely begin to affect a wider private industry audience as the National Institute of Standards and Technology (NIST) and Cybersecurity and Infrastructure Security Agency (CISA) begin releasing new guidance.

President Trump's Executive Order follows Executive Order 14144 (EO 14144), titled, "Strengthening and Promoting Innovation in the Nation's Cybersecurity," which President Biden signed on January 16, 2025, just before departing from office. EO 14144 remains

### Related People

- Sarah S. Glover
- Gregory J. Leighton
- Mary Ann H. Quinn

### Related Capabilities

- Executive Orders
- Privacy & Cybersecurity

one of the most comprehensive federal cybersecurity policy statements to date, aiming to fortify federal systems, enhance public-private collaboration on software security and proactively prepare for future technological threats like quantum computing and AI-driven attacks. Practically, it set forth a variety of specific instructions and deadlines for agencies to comply with and/or implement new cybersecurity initiatives and to amend the Federal Acquisition Regulation (FAR).

Given that it was signed four days before President Biden left office, EO 14144 was caught between administrations, and the future of many of its directives remained uncertain until recently. In large part, President Trump's recent Executive Order left EO 14144 intact, but it scaled back many of the deadlines and specific directives imposed on agencies, in the name of fostering flexibility and agency discretion. Importantly, the Executive Order underscores that cybersecurity remains a bipartisan concern, and federal priorities such as software supply chain security, improved cloud security, artificial intelligence, preparation for post-quantum computing and protection of space systems continue to be paramount. Below, we dive into the key provisions of President Trump's Executive Order, describe if or how they changed EO 14144's directives and analyze the impact to private industry.

## Secure Software Development Framework

Security in third-party software supply chains remains a priority in the new Executive Order. However, the Executive Order eliminates EO 14144's mandate for the federal government to implement secure software development attestation requirements into the FAR. EO 14144 would have required that contractors submit these attestations to CISA. EO 14144 would have also required a resource investment by CISA to develop a program where such attestations and supporting artifacts could be uploaded, audited and verified.

The new Executive Order cuts the attestation provisions and leaves only the requirement that by August 1, 2025, NIST establish a public-private consortium to develop guidance for the implementation of the Secure Software Development Framework (SSDF) outlined in NIST Special Publication 800-218. Following this consortium, the Executive Order requires NIST to update to the SSDF.

## FedRAMP Policies

Along with calling on various agencies to make cybersecurity enhancements to federal systems, EO 14144 also required that the FedRAMP director, together with NIST and CISA, develop policies and practices to incentivize cloud service providers in the FedRAMP marketplace to improve their baseline to meet these enhancements. President Trump's Executive Order leaves this directive in place. So, contractors providing cloud services to the federal government should prepare to see and match new FedRAMP guidelines.

## Securing Federal Communications

The Executive Order leaves in place the main components of EO 14144 related to secure internet routing, encryption of Domain Name System (DNS) traffic, planning for the transition to post-quantum cryptography and encrypting email messages in transport.

## Digital Identity Documentation

The one section from EO 14144 that President Trump's Executive Order eliminates entirely is the directive encouraging the federal government to require digital identity documents for individuals accessing public benefits programs. It also eliminates federal grant funding to assist states in developing digital identity documentation acceptance

programs.

## Promoting Security with and in Artificial Intelligence

President Trump's Executive Order revises EO 14144's approach to implementing AI initiatives. EO 14144 included a directive for various agencies to launch an AI pilot program on ways to use AI in vulnerability detection, automatic patch management and other areas of internal cybersecurity management. It also directed funding for these respective programs and required research on pre-determined topics such as human-AI interaction methods to assist defensive cyber analysis and for designing secure AI systems. The Executive Order scales back these specific measures and instead requires only that AI datasets be shared with the broader academic community and that certain agencies incorporate AI software into existing cybersecurity measures and interagency coordination mechanisms.

## Cyber Trust Mark Labeling

EO 14144 introduced the Cyber Trust Mark labeling program, and the new Executive Order continues this initiative. The Executive Order simplifies some of the directive but otherwise continues the requirement that the FAR be amended to state that agencies shall require vendors to adopt the Cyber Trust Mark label by January 4, 2027.

## Focusing on Foreign Threats

The Executive Order makes one additional revision to a prior order signed by President Obama, EO 13694, regarding the application of sanctions against persons engaged in malicious cyber activities. The Executive Order limits the application of sanctions in this context to "foreign persons," eliminating the possibility that such sanctions could be levied against US citizens.

## Conclusion

The primary thrust behind the Biden administration's EO 14144 remains intact after President Trump's Executive Order, which means that private industry should expect to see new rollouts of enhanced cybersecurity priorities regarding securing software supply chains, enhancing cloud security platforms and implementing new AI initiatives. Additionally, contractors can expect to see forthcoming updates to the FAR with respect to:

- Civil space cybersecurity contract requirements;
- Requirements for providers of internet routing technologies;
- Requirements for DNS providers for the federal government; and
- Cyber Trust Mark labeling requirements for providers of consumer internet-of-things devices.

For any questions about this Executive Order or to learn how Polsinelli can help with your cybersecurity compliance efforts and strategic initiatives, please contact the authors of this article.