Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Changes to National Cyber Policy in the Trump Administration

June 18, 2025

On June 6, 2025, the Trump Administration released Executive Order 14306 (E.O. 14306) titled *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144.* This E.O. marks a shift from previous administrations on cyber policy—and in particular, within the narrower area of cybersecurity policy. Where other administrations had previously sought greater consolidation of cybersecurity responsibilities at the federal level, E.O. 14306 seeks to redistribute these responsibilities among industry participants or remove the responsibilities altogether. This CRS Insight explores these changes in a historical context.

Background on Previous Federal Cyber Policy

Two decades ago, the federal government's cyber policy, in general, was largely centered around encouraging voluntary actions by the private sector and establishing public-private partnerships. While those are still tenets of the federal government's cybersecurity strategy, additional policies have supplemented or replaced previous ones to direct more specific actions from federal agencies and drive larger changes in the private sector. The Biden Administration's presidential actions were the most extensive set of policies, and sought to shift cybersecurity responsibilities away from each individual company toward those companies and entities that provide information technology (IT) goods and services (e.g., cloud service providers and software companies). It also established greater federal leadership on cybersecurity issues.

> ***Cyber versus Cybersecurity***
>
> *Cyber* is a broader term to refer to any information technology, system, network, data, or digital thing. *Cybersecurity* is a narrower term referring to the protection of an information technology, system, network, data or digital thing.

Executive Order 14144

Executive Order 14144 (E.O. 14144) titled *Strengthening and Promoting Innovation in the Nation's Cybersecurity* was released by the Biden Administration on January 16, 2025. It sought to build upon the cybersecurity work of Executive Order 14028, but since it was released in the waning days of the administration, many of its efforts did not start and/or were not taken up by the Trump Administration.

Congressional Research Service
https://crsreports.congress.gov
IN12570

Polices set forth in E.O. 14144 include

- mandates for the private sector to attest to secure software development practices when selling IT to the federal government;
- requirements for federal agencies to improve their own cybersecurity through greater threat-hunt operations and information sharing;
- directions for federal agencies to release guidance on mobile driver's licenses to spur their adoption;
- directions for federal agencies to begin deploying tools and accepting digital verification of identities;
- requirements for agencies to adopt post-quantum encryption;
- improvements to agency adoption of artificial intelligence (AI), particularly for safe applications and automating cybersecurity functions; and
- reductions in the thresholds the United States would use in issuing sanctions against individuals or entities that commit cyberattacks against U.S. interests.

Executive Order 13694

Executive Order 13694 (E.O. 13694) titled *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities* was released by the Obama Administration on April 1, 2015. It established the federal policies around using authorities granted by the International Emergency Economic Powers Act (IEEPA), the National Emergencies Act (NEA), and the Immigration and Nationality Act of 1952 (INA) to issue sanctions against malicious actors who use cyberspace to carry out their attacks. E.O. 13694 limited sanctions to "significant" events. E.O. 14144 removed that threshold.

Policies in E.O. 14306

The Trump Administration did not revoke previous cybersecurity executive orders, nor did it direct a review of prior ones, as was done with critical infrastructure security and resilience policy. Instead, E.O. 14306 kept the text from E.O. 14144 and E.O. 13694 in place and performed line edits to remove text or policies with which the administration disagrees. In doing so, the Administration established policies to reduce the involvement of federal agencies in shaping the nation's cybersecurity posture while also giving the private sector greater influence.

Policy changes include

- making explicit that sanctions can only be used against "foreign persons." This appears to be the existing policy as CRS was unable to find an example where sanctions were lodged against domestic persons for cyber-related violations, although a domestic person could be an individual or entity physically within the United States, regardless of citizenship or residency status;
- removing the requirement for government contractors to make attestations regarding their secure software development practices. Instead, contractors are encouraged to voluntarily adopt guidance from the National Institute of Standards and Technology (NIST) on cybersecurity practices;
- removing agency requirements to conduct digital identity work—including both work on mobile drivers' licenses and acceptance of digital identity verification;
- limiting agency AI work to improvements of cybersecurity automation; and

- reducing the requirements for adopting post-quantum cryptography.

Some policies persist across these executive orders:

- agencies are to adopt the Cyber Trust Mark program to ensure internet-of-things devices carry attestations of security;
- agencies are to manage cyber supply-chain risks pursuant to NIST guidance;
- agencies are to advance their cybersecurity practices, including through the use of threat-hunt operations and advanced cybersecurity tools; and
- agencies are to continue progress toward securing internet traffic and email communications.

Implications of Policy Changes

The President's nominees for the National Cyber Director and Director of the Cybersecurity and Infrastructure Security Agency are pending confirmation in the Senate. If confirmed, their potential work toward a new national cybersecurity strategy could provide greater detail on how agencies may implement administration priorities. Currently, the President's Budget for FY2026 and agency budgets offer some indications of how the Trump Administration is generally seeking to allocate cybersecurity resources—largely through reduced cybersecurity allocations at agencies.

Policymakers may choose to scrutinize both the executive order and the President's Budget as they pertain to congressional prerogatives, which could include

- implications for reduced investment in cybersecurity activities by agencies;
- the degree to which the private sector is positioned to act without federal direction and resources;
- the ability for agencies to manage nation-state cybersecurity threats;
- implications for reductions in agency programs and workforces both for near term and long-term objectives;
- the role of the federal government in spurring the adoption of new technologies; and
- how the nation shall employ AI technologies for cybersecurity.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer