Trump Administration Executive Order Changes Cybersecurity Policy





A new executive order from the Trump Administration is rewriting cybersecurity policy. According to a statement from the White House, this executive order seeks to amend "problematic elements of Obama and Biden-era Executive Orders." The statement specifically points to Executive Orders 14144 and 13694.

This order additionally strips "a mandate for U.S. government issued digital IDs" for undocumented immigrants that the administration believes "would have facilitated entitlement fraud and other abuse." It also strikes an Obama Administration policy that allowed sanctions against "any person" involved with foreign-directed hacking operations and states that now only a "foreign person" can be sanctioned.

This order also removes a Biden Administration requirement mandating that software developers submit attestations to validate their use of secure software development practices.

Below, security leaders share their insights on this order.

Security Leaders Weigh In

Dave Gerry, CEO at Bugcrowd:

This order walks away from important lessons. Rolling back secure by design software attestations and limiting sanctions to only foreign actors sends the wrong message at the wrong time. Those were put in place to reduce risk across the supply

chain. Also, narrowing sanctions to only apply to foreign actors leaves a clear gap, especially when we've seen domestic enablers working in lockstep with foreign adversaries.

The shift toward voluntary guidance sounds nice, however, in practice it often means slower adoption and fewer safeguards. It's hard to see how this makes us safer. Cybersecurity should be a nonpartisan commitment to national resilience – not a political bargaining chip.

Tim Mackey, Head of Software Supply Chain Risk Strategy at Black Duck:

With the executive actions that took place early in the current administration, it was notable that the cybersecurity executive orders from the previous administration were left untouched. With this new executive order, the current administration reverses the software attestation requirements established in OMB memo M23-16 which was authorized under EO14028. By modifying EO14144, which was an extension of EO14028 and built upon lessons learnt in industry, EO14028 is practically rescinded.

What we should expect to see is a more prescriptive set of guidance documents from NIST in 2025. By establishing a consortium with industry at the NCCoE, this executive order signals a desire by the administration to collaborate with industry on advancing the nations cybersecurity skills and competencies. With a focus on NIST publications SP800-218 and SP800-53, the administration recognizes that deploying secure software starts at development and ultimately cybersecurity success is based on securely deploying that software. Lastly, this order recognizes both the contributions open-source technologies bring to American innovation, but also the unique risks they pose.

https://www.securitymagazine.com/articles/101685-trump-administration-executive-order-changes-cybersecurity-policy