Lowenstein Sandler

Privacy & Cybersecurity

April 11, 2023

Biden Administration Aims to Shift Liability for Cyberattacks to Software Developers

By Kathleen A. McGee, Ken Fishkin, CISSP, CIPP/US, CIPM, CIPT, and Mikayla R. Berliner

In response to major cyber-related attacks caused by software security flaws, such as the SolarWinds breach, the Biden administration is gearing up to crack down on software providers that distribute products with security flaws that make customers vulnerable to cyberattacks.

One of the administration's objectives, as stated in its March 2023 National Cybersecurity Strategy, is to develop legislation to (1) shift liability for cyber breaches to software companies that "fail to take reasonable precautions to secure their software" and (2) prevent software companies "with market power" from fully disclaiming liability by contract.[1] The administration's stated goal is to "drive the market to produce safer products and services while preserving innovation and the ability of startups and other small- and medium-sized businesses to compete against market leaders."[2]

The administration plans to include a "safe harbor" that shields companies from liability if they take reasonable steps to "securely develop and maintain their software products and services."[3] The safe harbor will purportedly require best practices that are similar to those included in the National Institute of Standards and Technology (NIST) Secure Software Development Framework[4] and will evolve over time. This action will incentivize software developers to follow secure-by-design principles and perform prerelease testing, resulting in a greater level of security for both consumers and businesses.

The administration intends to convert these proposals into legislation with the assistance of both Congress and the private sector. In the interim, software developers should consider evaluating and updating their products and keep a close eye on what steps will be necessary to produce secure products and reduce liability for cyberattacks. Entities purchasing software products should also pay attention, as they may be able to seek compensation from software developers for cyberattacks.

---

[1] *National Cybersecurity Strategy*, The White House, pp. 20–21 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
[2] *Id.*
[3] *Id.*
[4] *See* Karen Scarfone, et al., *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities*, NIST (Feb. 3, 2022), https://www.nist.gov/publications/secure-software-development-framework-ssdf-version-11-recommendations-mitigating-risk.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

KEN FISHKIN, CISSP, CIPP/US, CIPM, CIPT
Manager of Information Security
T: 973.422.6748
kfishkin@lowenstein.com

MIKAYLA R. BERLINER
Associate
T: 862.926.6572
mberliner@lowenstein.com

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.

© 2023 Lowenstein Sandler LLP | One Lowenstein Drive, Roseland, NJ 07068 | +1 973.597.2500