

Biden signs executive order aiming to prevent future cybersecurity disasters

President Joe Biden signed an executive order on Wednesday implementing new policies aimed to improve national cybersecurity. The executive order comes in the wake of a number of recent cybersecurity catastrophes, such as last week's ransomware attack that took down the Colonial Pipeline, the Microsoft Exchange server vulnerabilities that may have affected north of 60,000 organizations, and the SolarWinds hack that compromised nine federal agencies late last year – each of which were specifically namedropped by the White House in a fact sheet accompanying the order.

The executive order outlines a number of initiatives, including reducing barriers to information sharing between the government and the private sector, mandating the deployment of multi-factor authentication in the federal government, establishing a Cybersecurity Safety Review Board modeled after the National Transportation Safety Board, and creating a standardized playbook for responding to “cyber incidents.” You can read more about all of the initiatives in the White House's fact sheet [here](#).

In the past few months, we've seen example after example of major IT systems breaking down, whether they allowed for a huge effort like the email server hack from the state-sponsored Chinese hacking group Hafnium (the White House promised a “whole of government response” to that one), a ransomware attack that forced public schools to cancel classes, or even a pair of breakdowns that appear to have

allowed workers to remote into their local water supply and mess things up. The policies outlined in Wednesday's executive order could create critical infrastructure to help prevent future cybersecurity disasters – or, at the very least, better limit any potential fallout.

<https://www.theverge.com/2021/5/12/22433266/biden-executive-order-cybersecurity-government-infrastructure-colonial-pipeline-solarwinds-hafnium>