The US Supreme Court Kneecapped US Cyber Strategy

After the Supreme Court limited the power of federal agencies to craft regulations, it's likely up to Congress to keep US cybersecurity policy intact.

TO PROTECT AMERICA'S vital infrastructure from hackers without relying on a moribund Congress, the Biden administration bet big on creative uses of existing laws. But the Supreme Court probably blew up that approach.

President Joe Biden's strategy relied on agencies interpreting the laws that give them regulatory powers to include cybersecurity, with the expectation that courts would defer to their interpretations of those laws under a decades-old legal doctrine known as Chevron deference.

But in a landmark case decided in late June, *Loper Bright Enterprises v. Raimondo*, the United States Supreme Court's conservative supermajority eliminated Chevron deference and ordered courts to determine for themselves what ambiguous laws say—without assigning nearly as much weight to agencies' interpretations.

Now, that controversial ruling could completely upend multiple agencies' plans to require better cybersecurity from critical infrastructure entities like hospitals, water systems, and power plants. It could even help corporate America overturn existing rules aimed at keeping hackers off cloud platforms, securing pipelines and airports, and improving disclosures of major breaches.

"There's the possibility of lawsuits to test the waters in a lot of regulations," says Harley Geiger, counsel with the Center for Cybersecurity Policy and Law. "It definitely becomes much more difficult

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

to regulate on critical infrastructure cybersecurity in areas where there is not sound or clear statutory backing."

Landmark Cyber Program Under Threat

Biden's marquee cyber regulation may also be his most endangered: a pending requirement for critical infrastructure organizations to report cyberattacks within 72 hours and ransomware payments within 24 hours.

The regulation, authorized by the 2022 Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), is meant to close massive gaps in the government's awareness of the cyberattacks plaguing US companies every day. But when the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) released the proposed rule in April, the business community slammed it for going further than lawmakers intended. By the time the public comment period closed earlier this month, many companies and trade groups had urged CISA to pare back the rule—with some of them even citing the *Loper Bright* ruling.

The criticism mostly focused on three aspects of the rule that could represent its biggest vulnerabilities in a future lawsuit: the definition of a "covered entity" subject to the reporting requirements, the definition of a "covered incident" that needs to be disclosed, and the list of information that needs to be reported. Businesses say CISA used much broader language for these three provisions than Congress intended.

"They have gone well beyond the text," says one cybersecurity-focused attorney, who requested anonymity because they represent clients in disputes with federal agencies. "There's a lot of vulnerable aspects to it."

Senate Homeland Security Committee chair Gary Peters, whose panel led the drafting of CIRCIA, added to the regulation's legal peril when

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

he filed a public comment saying that “the proposed rule is overbroad and needs additional clarity,” including on the definitions of covered incidents and covered entities. Peters’ objections are significant, because courts analyzing unclear laws will likely lean heavily on congressional intent.

It’s unclear if CISA will back down in the face of these headwinds. A spokesperson says the agency is “still assessing” the *Loper Bright* ruling “and any potential impacts that this may have on the agency’s rulemaking actions.” The spokesperson says the final regulation will be “consistent with authorities given to us by Congress.”

CISA officials “seem quite committed to the scope that they're aiming for, because they really seem to view it as important to their mission,” says Stephen Lilley, a partner at the law firm Mayer Brown who focuses on cyber matters. Even so, he added, “CISA now has to be thinking, have we pushed too far in light of these recent decisions, and do we need to be a bit more modest in our ambitions?”

The consequences of a government retreat are hard to predict but potentially serious. Scaled-back CIRCIA requirements could exempt more companies from reporting or reduce the amount of information they have to report, easing the burden on those organizations but weakening the government’s understanding of digital threats.

Most experts predict only modest changes. “I would expect them to try to make as limited a reaction as their lawyers say they need to make,” Lilley says.

Still, it’s clear that the officials behind the government’s biggest-ever cyber regulation—due to be finalized by October 2025—are on notice.

“There's no way that CISA takes the next [14] months to develop this rule without considering the effect of *Loper Bright* and the loss of Chevron deference,” Geiger says.

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

Planes, Trains, and Cloud Services

While CISA's incident reporting mandate has attracted the lion's share of post–*Loper Bright* attention, the ruling threatens a host of other existing and pending cyber regulations.

The Department of Health and Human Services is working on a rule that would condition hospitals' receipt of federal Medicare and Medicaid funding on their compliance with cyber requirements. The closely watched HHS rule represents the Biden administration's attempt to stem a massive tide of ransomware attacks on hospitals and the rest of the health care sector. But the powerful hospital industry has objected to new mandates, saying they will overly burden already struggling facilities. Few details are known about the rule—including its exact legal basis—so it's unclear whether HHS has been rewriting it to address *Loper Bright*.

Corporate America's most-loathed cyber regulation is the Securities and Exchange Commission's 2023 rule requiring publicly traded companies to announce cyber incidents with a "material" impact within four business days. That rule may be safe from new lawsuits, given the SEC's clear legal authority to require the disclosure of information that materially affects stock prices. But Geiger says companies might instead challenge the SEC's authority to penalize companies for hacks, since the underlying law and regulation don't mention cybersecurity. (The SEC declined to comment for this story.)

Lawsuits could also hit the Transportation Security Administration over its cyber requirements for pipeline, rail, and aviation operators. The TSA significantly modified its emergency directives to address industry criticism, but as the agency codifies those directives in more formal rules, disgruntled companies could seize the chance to sue. "There's not a history of that agency doing cyber, and there's not a great statutory hook to point to," says the cyber attorney, who cited "a lot of frustration" with the TSA's "perpetual invocation of an ongoing but

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

undescribed emergency" to justify the requirements. (The TSA declined to comment.)

The Commerce Department could hit a legal snag with its proposal to require cloud companies to verify their customers' identities and report on their activities. The pending rule, part of an effort to clamp down on hackers' misuse of cloud services, has drawn industry criticism for alleged overreach. A major tech trade group warned Commerce that its "proposed regulations risk exceeding the rulemaking authority granted by Congress." (Commerce declined to comment.)

Lawsuits could also target other regulations—including data breach reporting requirements from the Federal Trade Commission, the Federal Communications Commission, and financial regulators—that rely on laws written long before policymakers were thinking about cybersecurity.

"A lot of the challenges where the agencies are going to be most nervous [are] when they've been interpreting something for 20 years or they newly have interpreted something that's 30 years old," says the cyber attorney.

The White House has already faced one major setback. Last October, the Environmental Protection Agency withdrew cyber requirements for water systems that industry groups and Republican-led states had challenged in court. Opponents said the EPA had exceeded its authority in interpreting a 1974 law to require states to add cybersecurity to their water-facility inspections, a strategy that a top White House cyber official had previously praised as "a creative approach."

All Eyes on Congress

The government's cyber regulation push is likely to run headlong into a judicial morass.

Federal judges could reach different conclusions about the same regulations, setting up appeals to regional circuit courts that have very

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

different track records. “The judiciary itself is not a monolith,” says Geiger, of the Center for Cybersecurity Policy and Law. In addition, agencies understand cutting-edge tech issues much better than judges, who may struggle to parse the intricacies of cyber regulations.

There is only one real solution to this problem, according to experts: If Congress wants agencies to be able to mandate cyber improvements, it will have to pass new laws empowering them to do so.

“There is greater onus now on Congress to act decisively to help ensure protection of the critical services on which society relies,” Geiger says.

Clarity will be key, says Jamil Jaffer, the executive director of George Mason University’s National Security Institute and a former clerk to Supreme Court Justice Neil Gorsuch. “The more specific Congress gets, the more likely I think a court is to see it the same way an agency does.”

Congress rarely passes major legislation, especially with new regulatory powers, but cybersecurity has consistently been an exception.

“Congress moves very, very slowly, but it’s not completely passive [on] this front,” Lilley says. “There's a possibility that you will see meaningful cyber legislation in particular sectors if regulators are not able to move forward.”

One major question is whether this progress will continue if Republicans seize unified control of the government in November’s elections. Lilley is optimistic, pointing to the GOP platform’s invocation of securing critical infrastructure with heightened standards as “a national priority.”

“There's a sense across both sides of the aisle at this point that, certainly in some of the sectors, there has been some measure of market failure,” Lilley says, “and that some measure of government action will be appropriate.”

Regardless of who controls Capitol Hill next January, the Supreme Court just handed lawmakers a massive amount of responsibility in the fight against hackers.

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/

“It's not going to be easy,” Geiger says, “but it's time for Congress to act.”

https://www.wired.com/story/us-supreme-court-chevron-deference-cybersecurity-policy/