Easterly: Too early to say if Supreme Court's Chevron decision will affect cyber incident notification rules

LAS VEGAS – The head of the leading U.S. cybersecurity agency said it is too early to know whether its new rule on cyber incident reporting will be affected by a landmark Supreme Court decision limiting the power of regulators.

Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA), said her team is in the process of analyzing how their work will be affected by the June ruling, which saw the Supreme Court overturn the 1984 decision in Chevron v. Natural Resources Defense Council. The case gave rise to the "Chevron doctrine" — which said courts had to uphold regulatory agencies' power to interpret rules as they see fit if not specifically outlined by Congress.

In a 6-3 ruling in June, conservative justices on the Supreme Court struck down the doctrine, reigniting concerns that U.S. agencies will face a deluge of lawsuits from corporations eager to have certain rules removed.

At the Black Hat cybersecurity conference here on Wednesday, Easterly told Recorded Future News that her office is primarily analyzing how the ruling will impact the Cyber Incident Reporting for Critical Infrastructure Act, also known as CIRCIA, which will force certain critical infrastructure organizations to report cyberattacks to the federal government when it comes into effect.

"My team again is analyzing whether there will be any impacts from Chevron. I think it's too early for us to say but at the end of the day, I think it is so important to get this right, because this is not really traditional regulation at the end of the day," she explained.

"It is really about rendering assistance and using that information in an anonymized way to help protect a larger ecosystem and there's not really mechanisms for enforcement in the way that other regulations I've experienced, particularly in the financial sector."

While no federal cybersecurity regulations issued for critical sectors like railroads, airlines and pipelines have faced lawsuits so far in light of the Chevron ruling, some federal agencies have previously been forced to pull back cyber rules in response to legal attacks.

The Environmental Protection Agency (EPA) tried last year to add cybersecurity to an annual assessment done for water systems across the U.S. But the rules immediately faced lawsuits from Republican attorneys general and water industry groups — who all warned that the extra costs associated with increased cybersecurity protections would be passed on to customers.

The EPA eventually repealed the regulation after initial court rulings struck it down.

The Chevron ruling reignited concerns that industries chafing at increased cyber regulations would turn to courts as a method of circumventing new rules.

Easterly said on Wednesday that CIRCIA just finished the public comment phase and CISA is now going through the comments, analyzing them and making changes to the final rule — which Easterly said would be issued publicly late next year.

Easterly added that her goal was for entities that fall under CIRCIA to interpret it more as something they could benefit from as opposed to hard-and-fast regulation.

"I hope that when we finalize this rule, entities will say this is actually really useful because we are getting more information that is allowing us to protect our business because we understand how the other business got hacked," she said.

"There's a lot more work to do. I have a lot of optimism about what CIRCIA will ultimately portend for us to better understand the ecosystem of cyber incidents."

Tags CISA Jen Easterly regulation Supreme Court Critical Infrastructure Black Hat

Previous article

Royal ransomware successor BlackSuit has demanded...

Next article

Michigan hospital system struggles with cyberattack a...

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.