CYBERSECURITY DIVE

DIVE BRIEF

Congress adds historic cyber incident reporting rule to massive $1.5 trillion package

Key members of Congress and CISA say the bill will help protect critical infrastructure against malicious attacks.

Published March 11, 2022

David Jones
Reporter

onurdongel via Getty Images

Dive Brief:

- Congress passed landmark legislation Thursday that mandates critical infrastructure providers and federal agencies promptly report cyberattacks and ransomware payments to the Cybersecurity and Infrastructure Security Agency.
- The historic reporting requirements are part of a $1.5 trillion omnibus spending bill that President Joe Biden is expected to sign.
- CISA Director Jen Easterly praised the legislation in a statement Friday, noting her agency have better visibility and data to protect businesses and critical infrastructure.

Dive Insight:

Security experts have strongly advocated for reporting requirements following the 2020 supply chain attacks on

SolarWinds and the rash ransomware attacks on critical infrastructure providers, including Colonial Pipeline.

“CISA will use these reports from our private sector partners to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure,” Easterly said in the statement.

“This information will fill critical information gaps and allow us to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims,” she added.

The incident reporting legislation has been the subject of fierce debate within the information security community. Numerous companies have declined to notify federal agencies of prior ransomware and supply chain attacks prior to the SolarWinds nation-state attack and subsequent ransomware incidents.

Among the many concerns companies had were potential litigation from investors if companies incurred major costs as well as potential investigations from federal or state regulators.

Federal authorities have urged prompt notification so they could alert other potential targets. Investigations of the SolarWinds attack uncovered that threat actors were, in some cases, lurking in the systems of unsuspecting companies since late 2019, almost a year before the attack was uncovered in December 2020.

A major turf war recently erupted over which agency should receive the incident reports. The question centered on whether CISA should be the only mandated federal agency, or the FBI, which plays a central role in investigation and notification of ransomware and nation-state threats.

Katell Thielemann, Gartner Research VP said via email, “But as always, the devil will be in the details of implementation and in the outcomes that the reporting will support.”