



October 7, 2021

WHAT YOU NEED TO KNOW ABOUT

The Push for Mandatory Cyber Reporting

PRO POINTS

- **Major cyber incidents, including the Russian government's SolarWinds espionage campaign and the criminal ransomware attack on the Colonial Pipeline Co., have highlighted gaps in the government's understanding of digital threats.**
- **Key congressional committees have proposed requiring some companies to alert the federal government when they are hacked, but major differences exist between the leading bills.**
- **Time is running out for lawmakers to agree on a path forward because policymakers plan to tack the final product onto the too-big-to-fail fiscal 2022 defense policy bill, which needs to pass soon.**

HOW WE GOT HERE

The past year has been a whirlwind of sophisticated and disruptive cyberattacks. Ransomware gangs crippled the Colonial Pipeline Co. and the meat processing giant JBS, disrupting the U.S. fuel and food supplies, and used the IT services provider Kaseya as a springboard for attacks on hundreds of its business and government customers. Russian government hackers penetrated at least nine federal agencies and 100 businesses after infecting software made by the IT firm SolarWinds. And Chinese state operatives opened the door to a blizzard of attacks on Microsoft email servers by exploiting previously unknown vulnerabilities.

But those are just the attacks that have been discovered. Many potentially far-reaching hacks remain secret for months or years afterward because victims fear the reputational, financial or regulatory consequences of reporting them. This creates visibility gaps that make it harder for the government to assess the threat landscape and help protect companies that may be the hacker's next targets.

"We need to get that information as rapidly as possible, so that we can share it to prevent others from suffering," Jen Easterly, the director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, said at an industry conference on Sept. 29.

Key lawmakers in both chambers of Congress, convinced that recent hacks have highlighted an untenable situation, have drafted bills that would require certain companies to report breaches to the government. With support from Easterly and other senior Biden administration officials, Capitol Hill is on the verge of enacting one of the most significant cyber policies since the creation of the internet.

DIFFERING APPROACHES

Significant differences exist between the two major legislative efforts underway in Congress — and powerful industry groups have made it clear which approach they support.



The Senate Intelligence Committee's bill, introduced on July 21, would require federal contractors, critical infrastructure operators and cybersecurity companies to report both confirmed and potential breaches within 24 hours. Noncompliant companies could face daily fines of up to 0.5 percent of their most recent annual gross revenues.

The Senate Homeland Security Committee's bill, announced on Sept. 28, would only cover critical infrastructure operators, only require them to report confirmed hacks and give them at least 72 hours to do so. It would not create financial penalties, although it would authorize CISA to issue subpoenas for information and let the government sue companies that ignore those subpoenas. Noncompliant federal contractors could also lose their contracts.

The Senate Homeland bill is almost identical to a House Homeland Security Committee measure that lawmakers tucked into the fiscal 2022 National Defense Authorization Act, which passed the lower chamber on Sept. 23. It also includes several ransomware-specific provisions.

On all the key provisions — the reporting deadline, the scope of covered companies, the scope of covered incidents and the penalties for noncompliance — the private sector has lined up behind the homeland security panels.

WHAT'S NEXT

With the House having already approved an incident reporting mandate as part of the NDAA, the leaders of the Senate intelligence and homeland security committees are working on a compromise measure that would incorporate elements of both committees' bills.

But the fate of the program's most contentious elements remains unclear.

Senate Intelligence Chair Mark Warner (D-Va.) has indicated a willingness to narrow the scope of reported incidents, saying on Sept. 28 that "we don't want to overwhelm [CISA] with noise." He said he believed that "we're getting very close to a conclusion there."

But Warner may not budge on other lawmakers' demands to drop the financial penalties from the program. He called the homeland security panels' approach "toothless."



Biden administration officials could also play a key role in shaping the final product. Easterly has publicly backed Warner's approach of including cyber firms in the program and requiring notification within 24 hours.

But with the House already having passed a different kind of mandate in the NDAA, it's unclear whether the administration will push hard for the Warner approach, which would require the House to revisit the defense bill.



Key differences in cyberattack legislation introduced by Congress

Three congressional committees have proposed legislation to require companies to report cyberattacks. But the three bills take slightly different approaches to ensuring that the Cybersecurity and Infrastructure Security Agency has the necessary information to confront cyberattacks on U.S. critical infrastructure.

	 SENATE		 HOUSE
	INTELLIGENCE COMMITTEE	HOMELAND SECURITY COMMITTEE	HOMELAND SECURITY COMMITTEE
Which incidents need to be reported?	Confirmed and potential cyber incidents, with CISA creating more detailed criteria.	Only confirmed cyber incidents, with CISA creating more detailed criteria.	Only confirmed cyber incidents, with CISA creating more detailed criteria.
Which companies have to report incidents?	Federal contractors, critical infrastructure operators and cybersecurity service providers , with CISA creating more detailed criteria for which ones are covered.	Only critical infrastructure operators , with CISA creating more detailed criteria for which ones are covered.	Only critical infrastructure operators , with CISA creating more detailed criteria for which ones are covered
How quickly must companies report incidents?	Must be submitted within 24 hours of an incident.	CISA chooses a submission deadline of at least 72 hours and up to seven days after an incident.	CISA chooses a submission deadline of at least 72 hours after an incident.
INITIAL REPORTS			
FOLLOW UP REPORTS	Must be submitted within 72 hours of new developments.	CISA can set whatever deadline it wants.	CISA can set whatever deadline it wants.
RANSOM REPORTS		CISA chooses a submission deadline of between 24 and 72 hours after a payment.	
Can the government fine companies that don't comply?	Yes , the government can issue fines of up to 0.5 percent of the company's prior-year gross revenue per day of violation.	No	No
Can CISA subpoena companies if it suspects they've been hacked but they refuse to report information?	No	Yes, after three days of receiving no or inadequate information. The government can sue companies that defy these subpoenas.	Yes, after seven days of receiving no or inadequate information. The government can sue companies that defy these subpoenas. Also, subpoenaed companies lose the bill's liability and disclosure protections.

Source: POLITICO staff reports



POWER PLAYERS

- **Sen. Gary Peters:** The Senate Homeland Security chair controls the fate of any incident reporting legislation. Known for bipartisan efforts on cybersecurity, the Michigan Democrat has a heavy incentive to get something passed.
- **Sen. Rob Portman:** The Ohio Republican has sought bipartisan compromises on cybersecurity legislation. As a retiring senator, he faces less political pressure to appease the tech industry on this bill, but he may still sympathize with its feasibility concerns.
- **Sen. Mark Warner:** The moderate Virginia Democrat chairs the Intelligence Committee and is one of the upper chamber's most influential national security policymakers, but he risks being outmaneuvered by industry groups that have thrown their weight behind the Peters–Portman bill.
- **Sen. Susan Collins:** GOP support for a reporting mandate will be crucial in the narrowly divided Senate. The moderate Maine Republican, who co-sponsored the Senate Intelligence bill along with ranking member Sen. Marco Rubio, may be able to sway wavering colleagues.
- **Rep. Yvette Clarke:** As the chair of the House Homeland Security cyber subcommittee and the chief sponsor of her panel's bill, the eight-term New York Democrat has been a key voice in these legislative negotiations.
- **Rep. John Katko:** Katko, the ranking member on House Homeland Security Committee, is the lead Republican sponsor of the panel's bill. Generally considered a moderate, he is also an influential figure in GOP national security circles.