Massive breach fuels calls for US action on cybersecurity

February 19 2021, by Ben Fox and Alan Suderman

White House deputy national security adviser Anne Neuberger speaks during a press briefing, Wednesday, Feb. 17, 2021, in Washington. (AP Photo/Evan Vucci)

Jolted by a sweeping hack that may have revealed government and

corporate secrets to Russia, U.S. officials are scrambling to reinforce the nation's cyber defenses and recognizing that an agency created two years ago to protect America's networks and infrastructure lacks the money, tools and authority to counter such sophisticated threats.

The breach, which hijacked widely used software from Texas-based SolarWinds Inc., has exposed the profound vulnerability of civilian government networks and the limitations of efforts to detect threats.

It's also likely to unleash a wave of spending on technology modernization and cybersecurity.

"It's really highlighted the investments we need to make in cybersecurity to have the visibility to block these attacks in the future," Anne Neuberger, the newly appointed deputy national security adviser for cyber and emergency technology said Wednesday at a White House briefing.

The reaction reflects the severity of a hack that was disclosed only in December. The hackers, as yet unidentified but described by officials as "likely Russian," had unfettered access to the data and email of at least nine U.S. government agencies and about 100 private companies, with the full extent of the compromise still unknown. And while this incident appeared to be aimed at stealing information, it heightened fears that future hackers could damage critical infrastructure, like electrical grids or water systems.

President Joe Biden plans to release an executive order soon that Neuberger said will include about eight measures intended to address security gaps exposed by the hack. The administration has also proposed expanding by 30% the budget of the U.S. Cybersecurity and Infrastructure Agency, or CISA, a little-known entity now under intense scrutiny because of the SolarWinds breach.

Republicans and Democrats in Congress have called for expanding the size and role of the agency, a component of the Department of Homeland Security. It was created in November 2018 amid a sense that U.S. adversaries were increasingly targeting civilian government and corporate networks as well as the "critical" infrastructure, such as the energy grid that is increasingly vulnerable in a wired world.

Speaking at a recent hearing on cybersecurity, Rep. John Katko, a Republican from New York, urged his colleagues to quickly "find a legislative vehicle to give CISA the resources it needs to fully respond and protect us."

Biden's COVID-19 relief package called for $690 million more for CISA, as well as providing the agency with $9 billion to modernize IT across the government in partnership with the General Services Administration.

That has been pulled from the latest version of the bill because some members didn't see a connection to the pandemic. But Rep. Jim Langevin, co-chair of the Congressional Cybersecurity Caucus, said additional funding for CISA is likely to reemerge with bipartisan support in upcoming legislation, perhaps an infrastructure bill.

"Our cyber infrastructure is every bit as important as our roads and bridges," Langevin, a Rhode Island Democrat, said in an interview. "It's important to our economy. It's important to protecting human life, and we need to make sure we have a modern and resilient cyber infrastructure."

CISA operates a threat-detection system known as "Einstein" that was unable to detect the SolarWinds breach. Brandon Wales, CISA's acting director, said that was because the breach was hidden in a legitimate software update from SolarWinds to its customers. After it was able to

identify the malicious activity, the system was able to scan federal networks and identify some government victims. "It was designed to work in concert with other security programs inside the agencies," he said.

The former head of CISA, Christopher Krebs, told the House Homeland Security Committee this month that the U.S. should increase support to the agency, in part so it can issue grants to state and local governments to improve their cybersecurity and accelerate IT modernization across the federal government, which is part of the Biden proposal.

"Are we going to stop every attack? No. But we can take care of the most common risks and make the bad guys work that much harder and limit their success," said Krebs, who was ousted by then-President Donald Trump after the election and now co-owns a consulting company whose clients include SolarWinds.

The breach was discovered in early December by the private security firm FireEye, a cause of concern for some officials.

"It was pretty alarming that we found out about it through a private company as opposed to our being able to detect it ourselves to begin with," Avril Haines, the director of national intelligence, said at her January confirmation hearing.

Right after the hack was announced, the Treasury Department bypassed its normal competitive contracting process to hire the private security firm CrowdStrike, U.S. contract records show. The department declined to comment. Sen. Ron Wyden, D-Ore., has said that dozens of email accounts of top officials at the agency were hacked.

The Social Security Administration hired FireEye to do an independent forensic analysis of its network logs. The agency had a "backdoor code"

installed like other SolarWinds customers, but "there were no indicators suggesting we were targeted or that a future attack occurred beyond the initial software installation," spokesperson Mark Hinkle said.

Sen. Mark Warner, a Virginia Democrat who chairs the Senate Intelligence Committee, said the hack has highlighted several failures at the federal level but not necessarily a lack of expertise by public sector employees. Still, "I doubt we will ever have all the capacity we'd need in-house," he said.

There have been some new cybersecurity measures taken in recent months. In the defense policy bill that passed in January, lawmakers created a national director of cybersecurity, replacing a position at the White House that had been cut under Trump, and granted CISA the power to issue administrative subpoenas as part of its efforts to identify vulnerable systems and notify operators.

The legislation also granted CISA increased authority to hunt for threats across the networks of civilian government agencies, something Langevin said they were only previously able to do when invited.

"In practical terms, what that meant is they weren't invited in because no department or agency wants to look bad," he said. "So you know what was happening? Everyone was sticking their heads in the sand and hoping that cyberthreats were going to go away."