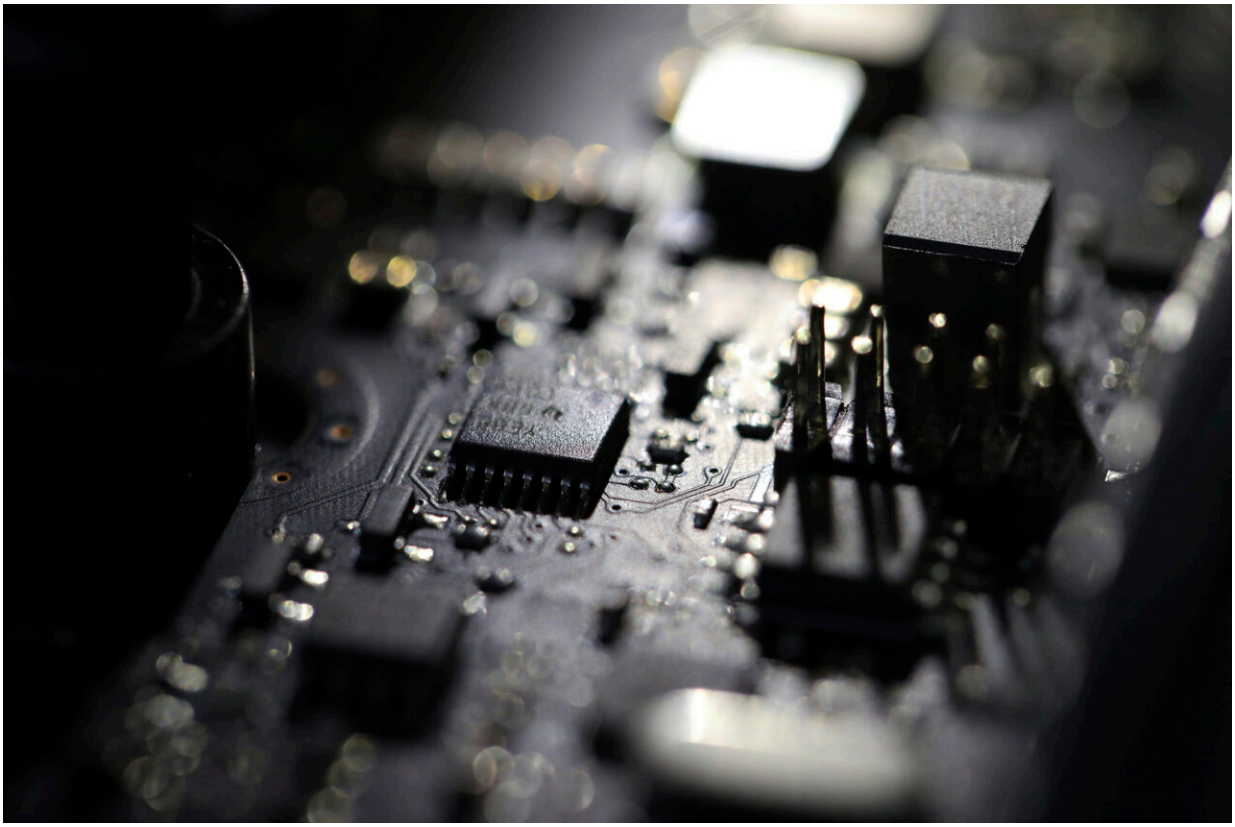
# Delay in creating new cybersecurity board prompts concern

January 25 2022, by Alan Suderman



This Feb 23, 2019, photo shows the inside of a computer. A key part of President Joe Biden's plans to fight major ransomware attacks and digital espionage campaigns has been languishing for more than eight months.Credit: AP Photo/Jenny Kane, File

It's a key part of President Joe Biden's plans to fight major ransomware

attacks and digital espionage campaigns: creating a board of experts that would investigate major incidents to see what went wrong and try to prevent the problems from happening again—much like a transportation safety board does with plane crashes.

But eight months after Biden signed an executive order creating the Cyber Safety Review Board it still hasn't been set up. That means critical tasks haven't been completed, including an investigation of the massive SolarWinds espionage campaign first discovered more than a year ago. Russian hackers stole data from several federal agencies and private companies.

Some supporters of the new board say the delay could hurt national security and comes amid growing concerns of a potential conflict with Russia over Ukraine that could involve nation-state cyberattacks. The FBI and other federal agencies recently released an advisory—aimed particularly at critical infrastructure like utilities—on Russian state hackers' methods and techniques.

"We will never get ahead of these threats if it takes us nearly a year to simply organize a group to investigate major breaches like SolarWinds," said Sen. Mark Warner, a Virginia Democrat who leads the Senate Intelligence Committee. "Such a delay is detrimental to our national security and I urge the administration to expedite its process."

Biden's order, signed in May, gives the board 90 days to investigate the SolarWinds hack once it's established. But there's no timeline for creating the board itself, a job designated to Department of Homeland Security Secretary Alejandro Mayorkas.

In response to questions from The Associated Press, DHS said in a statement it was far along in setting it up and anticipated a "near-term announcement," but did not address why the process has taken so long.

Scott Shackelford, the cybersecurity program chair at Indiana University and an advocate for creating a cyber review board, said having a rigorous study about what happened in a past hack like SolarWinds is a way of helping prevent similar attacks.

"It sure is taking, my goodness, quite a while to get it going," Shackelford said. "It's certainly past time where we could see some positive benefits from having it stood up."

The Biden administration has made improving cybersecurity a top priority and taken steps to bolster defenses, but this is not the first time lawmakers have been unhappy with the pace of progress. Last year several lawmakers complained it took the administration too long to name a national cyber director, a new position created by Congress.

The SolarWinds hack exploited vulnerabilities in the software supply-chain system and went undetected for most of 2020 despite compromises at a broad swath of federal agencies and dozens of companies, primarily telecommunications and information technology providers. The hacking campaign is named SolarWinds after the U.S. software company whose product was exploited in the first-stage infection of that effort.

The hack highlighted the Russians' skill at getting to high-level targets. The AP previously reported that SolarWinds hackers had gained access to emails belonging to the then-acting Homeland Security Secretary Chad Wolf.

The Biden administration has kept many of the details about the cyberespionage campaign hidden.

The Justice Department, for instance, said in July that 27 U.S. attorney offices around the country had at least one employee's email account

compromised during the hacking campaign. It did not provide details about what kind of information was taken and what impact such a hack may have had on ongoing cases.

The New York-based staff of the DOJ Antitrust Division also had files stolen by the SolarWinds hackers, according to one former senior official briefed on the hack who was not authorized to speak about it publicly and requested anonymity. That breach has not previously been reported. The Antitrust Division investigates private companies and has access to highly sensitive corporate data.

The federal government has undertaken reviews of the SolarWinds hack. The Government Accountability Office issued a report this month on the SolarWinds hack and another major hacking incident that found there was sometimes a slow and difficult process for sharing information between government agencies and the private sector, The National Security Council also conducted a review of the SolarWinds hack last year, according to the GAO report.

But having the new board conduct an independent, thorough examination of the SolarWinds hack could identify inconspicuous security gaps and issues that others may have missed, said Christopher Hart, a former National Transportation Safety Board chairman who has advocated for the creation of a cyber review board.

"Most of the crashes that the NTSB really goes after ... are ones that are a surprise even to the security experts," Hart said. "They weren't really obvious things, they were things that really took some deep digging to figure out what went wrong."