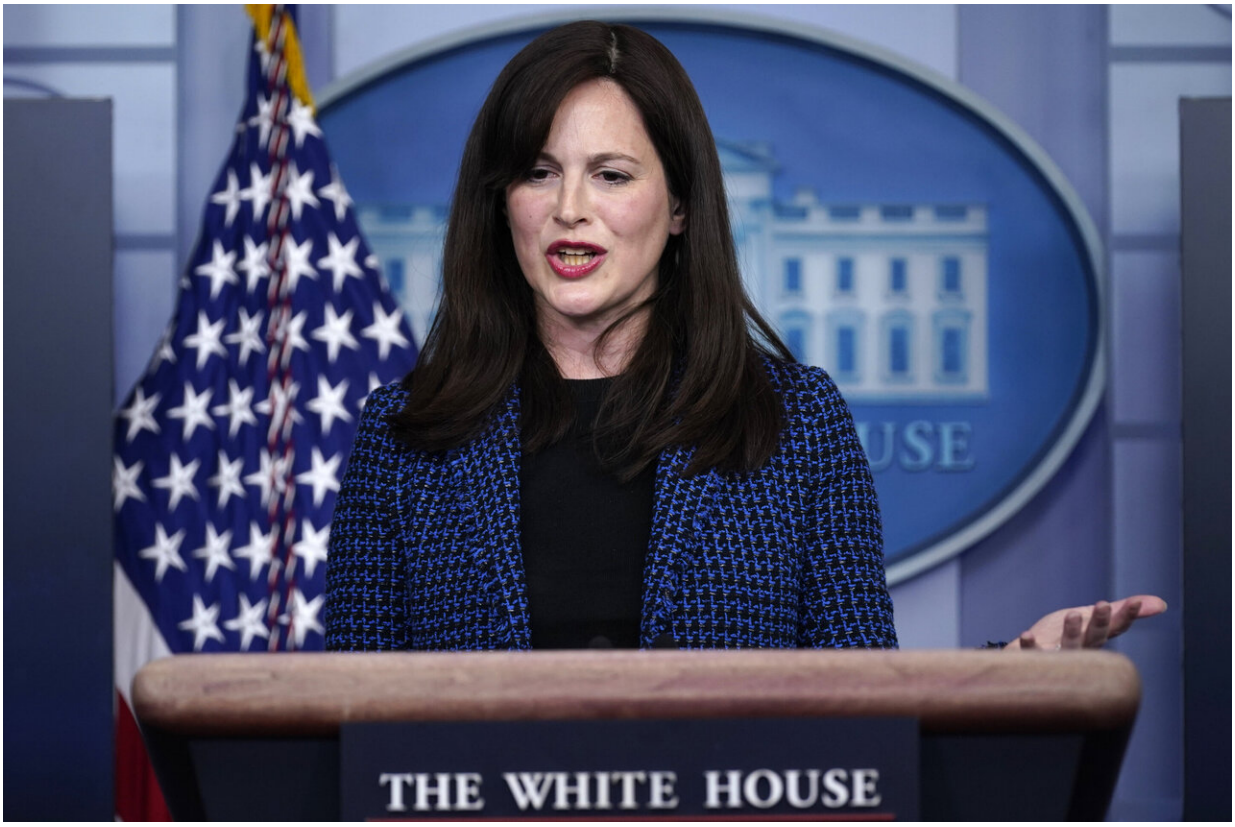
US looks to keep critical sectors safe from cyberattacks

April 2 2021, by Eric Tucker and Alan Suderman



In this Feb. 17, 2021, file photo White House deputy national security adviser Anne Neuberger speaks during a press briefing in Washington. The Biden administration has created an initiative aimed at helping critical industries, like the electric utility and water sectors, protect against damaging and destabilizing cyberattacks. "Our aim is to ensure that control systems serving 50,000 or more Americans have the core technology to detect and block malicious cyber activity," Neuberger said in an interview with The Associated Press on Thursday, April 1. (AP Photo/Evan Vucci, File)

A top Biden administration official says the government is undertaking a new effort to help electric utilities, water districts and other critical industries protect against potentially damaging cyberattacks.

"Our aim is to ensure that control systems serving 50,000 or more Americans have the core technology to detect and block malicious cyber activity," Anne Neuberger, deputy national security adviser, said in an interview with The Associated Press on Thursday. "That's it in a sentence. Clear, clean goal, but it's going to take a lot of work to get there."

The public-private partnership reflects the administration's concerns about the vulnerability of vital systems, including the electric grid and water treatment plants, to hacks that could cause catastrophic consequences to American life. Though there is a history of government working with utilities, officials believe the threat has increased as more utility systems are connected to the Internet, and the Biden administration wants to make fast progress in blocking any attacks.

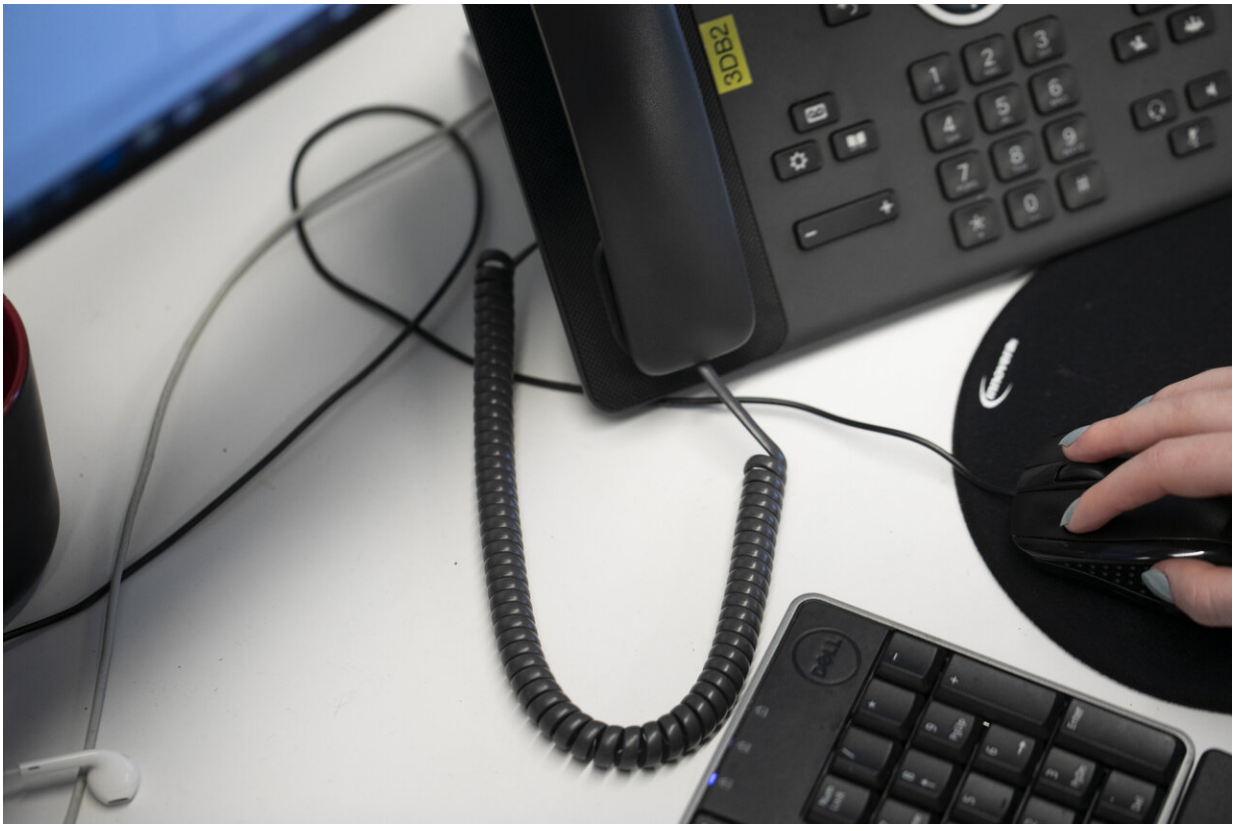
The administration, meanwhile, has grappled in its first 60 days with responses to two major cyber intrusions. In the first, Russian hackers snuck malicious code into a software update pushed out to thousands of government agencies and private companies. The second even more widespread hack affected untold thousands of Microsoft Exchange email servers, a breach the company says was carried out by Chinese state hackers.

Microsoft created a single -click tool to fix the issue after the White House encouraged the company to find a simple method for cleaning up from the hack. As a result, the number of compromised systems fell from 100,000 to less than 10,000 and "it keeps dropping," Neuberger

said.

She said one idea that was contemplated was whether Microsoft could push a patch to all compromised systems to effectively "vaccinate" them. Though it was determined that that was not technically feasible in this case, the government will continue to work with the private sector to explore that idea in future cases.

Neuberger is also the administration's point person in responding to the so-called SolarWinds hack, in which suspected Russian hackers breached at least nine different federal agencies. The AP reported this week that the hackers gained access to email accounts belonging to the Trump administration's head of the Department of Homeland Security and members of the department's cybersecurity staff whose jobs included hunting threats from foreign countries.



In this Oct. 8, 2019, file photo a woman works at a computer in New York. The Biden administration is not planning to step up government surveillance of the U.S. internet even as state-backed foreign hackers and cybercriminals increasingly use it to evade detection, a senior administration official said Friday. (AP Photo/Jenny Kane, File)

Neuberger said there were "gaps" in basic cybersecurity defenses at some of the nine agencies affected, which has hampered officials' ability to determine what the hackers accessed.

She said the administration has identified five specific modernization efforts as a result of its review of how the SolarWinds hack happened, including using technology that continuously monitors for malicious activity and requiring greater use of multi-factor authentication so systems can't be accessed with a stolen password alone.

That threat to critical infrastructure was laid bare in February after a hacker's botched attempt to poison the water supply of a small Florida city raised alarms about how vulnerable the nation's utilities may be to attacks by more sophisticated intruders.

A local sheriff said that the water supply of Oldsmar, population 15,000, was briefly in danger when an unknown hacker used a remote access program shared by plant workers to briefly increased the amount of lye—sodium hydroxide—by a factor of 100. Lye is used to lower acidity, but in high concentrations it is highly caustic and can burn. It's found in drain cleaning products.

A supervisor monitoring a plant console about 1:30 p.m. saw a cursor

move across the screen and change settings and was able to immediately reverse it. The intruder was in and out in five minutes. Suspicious incidents are rarely reported and usually are chalked up to mechanical or procedural errors, experts say. No federal reporting requirement exists, and state and local rules vary widely.

The nation's 151,000 public water systems lack the financial fortification of the corporate owners of nuclear power plants and electrical utilities. They are a heterogenous patchwork, less uniform in technology and security measures than in other rich countries.

On Wednesday, federal prosecutors charged a Kansas man who they said accessed a rural water district's protected computer system without authorization and "performed activities that shut down the processes at the facility which affect the facilities cleaning and disinfecting procedures."