THE NATIONAL LAW JOURNAL
FEBRUARY 10, 2021
An ALM Publication

What's to Come for Cybersecurity in the Biden Era

Recent developments offer early answers to what the Biden administration's cybersecurity policy will look like (while, at the same time, raising important questions).

BY **ALEXANDER H. SOUTHWELL AND DANIEL RAUCH**

Last month, in response to the SolarWinds hack, then-President-elect Joe Biden offered a simple message: "We will respond and probably respond in kind." For campaign observers, such tough talk might be unsurprising; Biden ran, after all, on a platform of "deter[ring] cyber threats" and "demand[ing] … countries cease and desist from conducting cyberespionage."

Signage outside SolarWinds Corp. headquarters in Austin, Texas. Photo: Bronte Wittpenn/Bloomberg

In its first weeks, the administration has matched strong words with strong actions: elevating veteran cybersecurity leaders, calling for vast digital defense investments and laying the groundwork for renewed cooperation with allies abroad and the private sector at home. Together, these developments offer early answers to what the Biden administration's cybersecurity policy will look like (while, at the same time, raising important questions).

Strong Leaders and a Deep Bench

With its first hires, the Biden administration has made clear that cybersecurity will be front and center. For national cyber director, a new role established by the 2021 National Defense Authorization Act, the president has tapped Jen Easterly, a former National Security Agency official who helped create U.S. Cyber Command. The National Security Council will include at least five experienced cybersecurity officials, including Anne Neuberger, who will serve as deputy national security adviser for cyber and emerging technology (a newly created role meant to elevate the subject internally and coordinate cybersecurity efforts across the government).

And they aren't alone. Vice President Kamala Harris and Health and Human Services Secretary nominee Xavier Becerra each served as California Attorney General, and each made cybersecurity and data privacy priorities

in that role. Avril Haines, now director of national intelligence, has extensive cybersecurity experience. And Biden's pick to lead the Department of Homeland Security, Alejandro Mayorkas, was previously deputy DHS secretary, with a portfolio including addressing diverse cyber threats and negotiating a key cybersecurity agreement with China.

"Surging" Resources

The president's spending priorities have also reflected his pledge to make cybersecurity a "top priority." In his American Rescue Plan stimulus proposal, Biden asks Congress for $10 billion for "the most ambitious effort ever to modernize and secure federal IT and networks." The centerpiece of this effort is a $9-billion request for IT and cybersecurity shared services at the General Services Administration and Cybersecurity and Infrastructure Security Agency. The plan also calls for $690 billion for "cybersecurity across federal civilian networks"; $300 million for GSA Technology Transformation Services programs; and $200 million to "surge cybersecurity technology and engineering expert hiring." This commitment is impressive in both absolute and relative terms. For instance, the plan requests $10 billion for pandemic supply manufacturing and $20 billion for a national vaccine distribution program—comparable sums. This sends a powerful signal: even in a pandemic, technological security may be as important as medical security.

Building Bridges

Along with surging personnel and money, this administration seems likely to look to cooperation, both with other nations and the private sector, as a key part of its cybersecurity approach. Early signs include a thaw with European Union officials, who view the Biden administration as more receptive to cybersecurity cooperation, the appointment of officials with cyber-diplomacy experience (like Mayorkas), and a renewed focus on working with the private sector.

What's Next?

Even as the administration's opening moves have answered some questions, they raise others:

- Will cooperation prevail? One of Biden's core messages, in the campaign and after, has been a plea for bipartisan unity. Cybersecurity policy could be a big part of this vision, as cross-party cooperation has historically been possible on a variety of cybersecurity issues. Alternatively, it is also possible that cybersecurity, like many other issues, may cause continued fractures, especially if the focus shifts from areas of consensus and toward controversial issues like Section 230 immunity.
- How far "forward" will cyber defenses lean? In recent years, as crystallized in a 2018 Department of Defense Cyber Strategy document, America's approach to cybersecurity has leaned toward "defend forward" (i.e., the best cyber defense is one that addresses threats as close as possible to their source), and "persistent engagement" (i.e., favor proactive, offensive actions to take the initiative). It is possible Biden may double down on this offense-minded approach. Yet this posture is not without controversy, and in time, we may see a less hawkish strategy, with emphasis shifting toward cooperation, diplomacy and "passive" defenses.
- What role will the private sector play? As former DHS cybersecurity official Mark Weatherford recently observed, "20 years ago, dealing with foreign nation attacks were the sole responsibility of the federal government," but today, private companies are prime targets of well-resourced, state-sponsored attacks. In this context, a key question is whether, and to what extent, the Biden administration's early promises of private-sector cooperation will be realized. If they are, the private sector may have opportunities for unprecedented government funding, expertise and operational support. At the same time, we expect increased regulatory scrutiny of companies' cybersecurity posture, as well as privacy practices, particularly those companies contracting with the government and in the information technology supply chain. Such a rise of intense regulatory scrutiny might prove to be at odds with governmental cooperation, and companies will have to navigate that tension, even as they devote more resources and attention to cybersecurity defenses.

And of course, given the fluid, ever-changing nature of the threat, it may well be an "unknown unknown"—dangers we did not know we did not know—that comes to define the next four years. The early answers are now clear. The questions are just getting started.

Alexander H. Southwell *co-chairs Gibson, Dunn & Crutcher's privacy, cybersecurity and consumer protection practice group and is a former federal cyber-crimes prosecutor. Former associate Daniel Rauch is a Denver lawyer.*