The Washington Post
Democracy Dies in Darkness

U.S. national cyber strategy to stress Biden push on regulation

The White House wants expanded requirements for private companies that operate in critical infrastructure sectors

By Ellen Nakashima and Tim Starks
January 5, 2023 at 6:00 p.m. EST

The Biden administration is set to unveil a national strategy that for the first time calls for comprehensive cybersecurity regulation of the nation's critical infrastructure, explicitly recognizing that years of a voluntary approach have failed to secure the nation against cyberattacks, according to senior administration officials.

The strategy builds on the first-ever oil and gas pipeline regulations imposed last year by the administration after a hack of one of the country's largest pipelines led to a temporary shutdown, causing long lines at gas stations and fears of a fuel shortage. The attack on Colonial Pipeline by Russian-speaking criminals elevated ransomware to an issue of national security.

The strategy, drawn up by the White House Office of the National Cyber Director (ONCD), is moving through the final stages of interagency approval — involving more than 20 departments and agencies — and is expected to be signed by President Biden in the coming weeks, according to the officials, who spoke on the condition of anonymity because the document is not yet public.

"It's a break from the previous strategies, which focused on information sharing and public-private partnership as the solution," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies think tank. "This goes well beyond that. It says things that others have been afraid to say."

For instance, according to a draft copy of the strategy, one of the stated goals is: "Use Regulation to support National Security and Public Safety." Under that, it says that regulation "can level the playing field" to meet the needs of national security, according to two individuals familiar with the draft.

It also states that "while voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has too often resulted in inconsistent and, in many cases inadequate, outcomes."

It even calls for shifting liability "onto those entities that fail to take reasonable precautions to secure their software" while recognizing that even the most advanced software security programs cannot prevent all vulnerabilities.

"If 'tough' means that we have to be serious about what we want cyberspace to do for us … then it's time for us to be tough," National Cyber Director Chris Inglis said at a cyber conference hosted by Cipher Brief, a national security analysis site, in September. "If at the end of the day, self-enlightenment and market forces take us [only] so far … then we have to go a little bit further as we have for cars, or airplanes, or drugs and therapeutics."

The strategy calls for regulation of all critical sectors — either by executive authority, as with pipelines, or by a congressional action where executive authority is lacking, the officials said.

Following the Colonial Pipeline incident, the White House National Security Council under the direction Anne Neuberger, deputy national security adviser for cyber and emerging technology, undertook an analysis of the state of regulation for all 16 critical infrastructure sectors. The result was instructive.

Five of them — nuclear power, financial services, large energy generation, chemicals and major defense contractors — had some form of cybersecurity regulations in place, imposed over the years before the Biden administration. After the Colonial hack, regulations were imposed on several more: oil and gas pipelines, rail and aviation. Soon the Environmental Protection Agency will issue a rule for the water sector, one of the senior officials said.

But the analysis also found there are five critical sectors of the U.S. economy in which oversight agencies lack authority to issue national-level cyber regulation. Those include food and agriculture, government facilities such as election infrastructure and schools, and "critical manufacturing" — including vaccine-makers, pharmaceuticals and mask manufacturers, the official said. That's where Congress would have to step in to pass legislation granting the relevant federal agency power to regulate, the official said.

The analysis looked at the companies in each sector for impact on Americans' lives in the case of a disruption, because shutting down a major electric power generation company affects many more Americans than a small one. So, for instance, only 97 of the largest pipeline companies — those serving 50,000 or more customers or transporting hazardous materials — were covered by last year's regulation, the official said.

"That's another key part of the approach, which is to say this doesn't apply to everyone," said Neuberger at a Washington Post Live event in October. "A careful look by the sector lead agency who understands the sector, who says who are the big players, who are the players who a disruption of their services would impact Americans broadly … those are the ones we're focused on."

The National Security Council analysis is reflected in the strategy, and there will be a separate implementation plan that is still being worked on, officials said.

The strategy directs that regulations need to be developed in consultation with industry — to ensure that the rules advance security without being unworkable or unduly burdensome. The officials conceded that, for instance, the first attempt at setting pipeline rules last year failed because they were done in haste and without consulting the companies, and as a result were overly prescriptive. “It wasn’t done right,” a second official said.

The first set of rules were “massively a bust,” said Robert M. Lee, chief executive of the industrial cybersecurity firm Dragos, which helps pipeline companies harden their operational systems against hacks. “Even attempting them would have caused disruptions to systems. They were asking for things that were technically not feasible.”

The second set was much improved, he said. “It took in pipeline asset and owner feedback. They moved towards more performance-based, than prescriptive standards: ‘Here’s what we want you to accomplish,’ not ‘here’s how to accomplish it.’”

The U.S. Chamber of Commerce, which spends the most of any lobbying organization in the United States, drove a successful campaign a decade ago to kill legislation that would have mandated cybersecurity standards. Cognizant that the political winds have shifted in the wake of Colonial Pipeline and Russia’s invasion of Ukraine — which prompted fears that Moscow might hack American critical infrastructure — it has moderated its stance slightly, accepting that regulations are inevitable but seeking some incentives to encourage compliance.

In a statement to The Post, the Chamber asserted that it shares “a mutual interest” with Inglis’s office — the ONCD — in “advancing regulatory harmonization, liability protections and federal preemption.”

Harmonization means, for instance, avoiding multiple agencies conducting cybersecurity inspections on the same company. “Liability protections” is an apparent reference to immunity, for instance from lawsuits, if certain standards are met, and “federal preemption” means ensuring that a national-level regulation supersedes state rules so that companies are not subject to a patchwork quilt of requirements.

“I’m glad to see the Chamber recognized that we need some federal baselines,” said Jeff Greene, who until July led the NSC cyberdefense policy and is now with the Aspen Institute think tank. “It’s a step in the right direction.”

States have authority to regulate electric power distribution, and New York Gov. Kathy Hochul (D) just last month signed legislation imposing cybersecurity rules on the state’s energy distribution grid. The news release noted that the action followed a request from Biden that states set minimum cybersecurity requirements for critical infrastructure, including the energy system.

“The strategy reflects the hard lessons we’ve learned from SolarWinds [the Russian hack of U.S. agencies] to Colonial Pipeline — that our supply chain and our critical infrastructures are under duress,” said Mark Montgomery, senior fellow at the Foundation for Defense of Democracies. “But the hard part comes next, translating all the good ideas into action.”