White House Cybersecurity Strategy Stresses Software Safety

An ambitious and wide-ranging White House cybersecurity plan released Thursday calls for bolstering protections on critical sectors and making software companies legally liable when their products don’t meet basic standards. The strategy document promises to use “all instruments of national power” to pre-empt cyberattacks.

The Democratic administration also said it would work to “impose robust and clear limits” on private sector data collection, including of geolocation and health information.

“We still have a long way to go before every American feels confident that cyberspace is safe for them,” acting national cyber director Kemba Walden said during an online forum on Thursday. “We expect school districts to go toe-to-toe with transnational criminal organizations largely by themselves. This isn’t just unfair. It’s ineffective.”

The strategy largely codifies work already underway during the last two years following a spate of high-profile ransomware attacks on critical infrastructure. A 2021 attack on a major fuel pipeline caused panic at the pump, resulting in an East Coast fuel shortage, and other damaging attacks made cybersecurity a national priority. Russia’s invasion of Ukraine compounded those concerns.

The 35-page document lays the groundwork for better countering rising threats to government agencies, private industry, schools, hospitals and other vital infrastructure that are

routinely breached. In the past few weeks, the FBI, U.S. Marshals Service and Dish Network were among the intrusion victims.

“The defense is hardly winning. Every few weeks someone gets hacked terribly,” said Edward Amoroso, CEO of the cybersecurity firm TAG Cyber.

He called the White House strategy largely aspirational. Its boldest initiatives – including stricter rules on breach reporting and software liability – are apt to meet resistance from business and Republicans in Congress.

Brandon Valeriano, former senior adviser to the federal government’s Cyberspace Solarium Commission, agreed.

“There’s a lot to like here. It just lacks a lot of specifics,” said Valeriano, a distinguished senior fellow at the Marine Corp. University. “They produce a document that speaks very much to regulation at a time when the United States is very much against regulation.”

The strategy’s data-collection component is also expected to meet stiff headwinds in Congress, though opinion polls say most Americans favor federal data privacy legislation.

In a new report, the tech data firm Forrester Research said state-sponsored cyberattacks rose nearly 100% between 2019 and 2022 and their nature changed, with a greater percentage now carried out for data destruction and financial theft. The threats are mostly from abroad: Russia-based cybercrooks and state-backed hackers from Russia, China, North Korea and Iran.

President Joe Biden’s administration has already imposed cybersecurity regulations on certain critical industry sectors, such as electric utilities, gas pipelines and nuclear facilities. The strategy calls for expanding them to other vital sectors.

In a statement accompanying the document, Biden says his administration is taking on the “systemic challenge that too much of the responsibility for cybersecurity has fallen on individual users and small organizations.” That will mean shifting legal liability onto software makers, holding companies rather than end users accountable.

As a nation, “we tend to devolve responsibility for cybersecurity downward. We ask individuals, small businesses and local governments to shoulder a significant burden for defending us all,” Walden said.

The White House wants to put greater responsibility on the software companies.

“Too many vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown provenance,” the document says. That must change, it adds, stating that the White House will work with Congress and the private sector on legislation to establish liability.

The director of the Cybersecurity and Infrastructure Security Agency, Jen Easterly, drew an analogy in a speech Monday at Carnegie Mellon University to the automotive industry before consumer advocates led by Ralph Nader forced safety reforms, including seat belts and air bags: “The burden of safety should never fall solely upon the customer. Technology manufacturers must take ownership of the security outcomes for their customers.”

But Amoroso, the cybersecurity executive, called that comparison misguided because software is a different animal, inherently complex with hackers constantly finding ways to break it. The liability initiative is apt to get tied up in the courts as industry resists, he said. “If you are a cybersecurity lawyer this is manna from heaven.”

Asked if it was fair to make software companies liable in court for cyberattack damage, the trade association BSA – The Software Alliance said in a statement: “Cybersecurity is constantly evolving and providing incentives for companies to use best practices in secure software design and development would benefit the entire ecosystem.”

The group, whose members include Microsoft, Adobe, SAP, Oracle and Zoom, added: “We look forward to working with the administration and Congress on any proposed legislation to promote best practices.” Amoroso said he liked positive aspects of the strategy such as securing clean-energy technologies and bolstering the cybersecurity work force, currently short 700,000 workers nationally.

The document also calls for more aggressive efforts to pre-empt cyberattacks by drawing on military, law enforcement and diplomatic tools as well as help from the private sector. Such offensive operations, it says, must take place with “greater speed, scale, and frequency.”

Disruption of hostile cyberactivity through “defending forward” is already happening.

The FBI and U.S. Cyber Command now routinely engage cybercriminals and state-backed hackers in cyberspace, working with foreign partners to thwart ransomware operations and election interference in 2018 and 2020. The government has already deemed ransomware a national security threat and the document says it will continue to use methods such as “hacking the hackers” to combat it.

Related: A Deeper Dive Into Zero-Trust and Biden’s Cybersecurity Executive Order

White House Cybersecurity Strategy Stresses Software Safety