President Trump has reversed an Obama-era memorandum dictating how and when the U.S. government can deploy cyberweapons against its adversaries, in an effort to loosen restrictions on such operations, according to people familiar with the action.

Mr. Trump signed an order on Wednesday reversing the classified rules, known as Presidential Policy Directive 20, that had mapped out an elaborate interagency process that must be followed before U.S. use of cyberattacks, particularly those geared at foreign adversaries.
The change was described as an “offensive step forward” by an administration official briefed on the decision, one intended to help support military operations, deter foreign election influence and thwart intellectual property theft by meeting such threats with more forceful responses.

The Trump administration has faced pressure to show that it is taking seriously national-security cyberthreats—particularly those that intelligence officials say are posed by Moscow.

Top administration officials are also devising new penalties that would allow stronger responses to state-sponsored hacks of U.S. critical infrastructure, The Wall Street Journal reported earlier this month, a mounting worry due to Russia’s efforts to penetrate American electric utilities.

Although the Obama-era policy was classified, its contents were made public when it was leaked in 2013 by former intelligence contractor Edward Snowden. It was signed by Mr. Trump’s predecessor, President Obama, in 2012.

It wasn’t clear what rules the administration is adopting to replace the Obama directive. A number of current U.S. officials confirmed the directive had been replaced but declined to comment further, citing the classified nature of the process.

Some lawmakers have raised questions in recent months about whether U.S. Cyber Command, the chief agency responsible for conducting offensive cyber missions, has been limited in its ability to respond to alleged Russian efforts to interfere in U.S. elections due to layers of bureaucratic hurdles.

The policy applies to the Defense Department as well as other federal agencies, the administration official said, while declining to specify which specific agencies would be affected. John Bolton, Mr. Trump’s national security adviser, began an effort to remove the Obama directive when he arrived at the White House in April, the official said.

As designed, the Obama policy required U.S. agencies to gain approval for offensive operations from an array of stakeholders across the federal government, in part to avoid interfering with existing operations such as digital espionage.

Critics for years have seen Presidential Policy Directive 20 as a particular source of inertia, arguing that it handicaps or prevents important operations by involving too many federal agencies in potential attack plans. But some current and former U.S. officials have expressed
concern that removing or replacing the order could sow further uncertainty about what offensive cyber operations are allowed.

One former senior U.S. official who worked on cybersecurity issues said there were also concerns that Mr. Trump’s decision will grant the military new authority “which may allow them to have a domestic mission.”

The Obama directive, which replaced an earlier framework adopted during the George W. Bush administration, was “designed to ensure that all the appropriate equities got considered when you thought about doing an offensive cyber operation,” said Michael Daniel, who served as the White House cybersecurity coordinator during the Obama administration. “The idea that this is a simple problem is a naive one.”

“If you don’t have good coordination mechanisms, you could end up having an operation wreck a carefully crafted multiyear espionage operation to gain access to a foreign computer system,” added Mr. Daniel, now president and CEO of the Cyber Threat Alliance, a cybersecurity nonprofit.

Several U.S. officials familiar with the Obama-era directive conceded the rules had flaws, but said that rescinding them could create more problems, especially because the administration hasn’t spelled out a replacement.

“I am sympathetic to trying to make our cyber capabilities more nimble in their use,” said Joshua Geltzer, who was senior director of counterterrorism at the National Security Council until March of last year. “On the other hand, there were some very real and hard legal questions associated with cyber about what operations the government would take that still have not been resolved.”

—Shelby Holliday contributed to this article.

Appeared in the August 16, 2018, print edition as ‘Cyberattack Rules Go on the Offensive.’