WASHINGTON -- The Obama administration plans to create a new military command to coordinate the defense of Pentagon computer networks and improve U.S. offensive capabilities in cyberwarfare, according to current and former officials familiar with the plans.

The initiative will reshape the military’s efforts to protect its networks from attacks by hackers, especially those from countries such as China and Russia. The new command will be unveiled within the next few weeks, Pentagon officials said.

The move comes amid growing evidence that sophisticated cyberspies are attacking the U.S. electric grid and key defense programs. A page-one story in The Wall Street Journal on Tuesday reported that hackers breached the Pentagon’s biggest weapons program, the $300 billion Joint Strike Fighter, and stole data. Lawmakers on the House Oversight and Government Reform Committee wrote to the defense secretary Tuesday requesting a briefing on the matter.

Lockheed Martin Corp., the project’s lead contractor, said in a statement Tuesday that it believed the article "was incorrect in its representation of successful cyber attacks" on the F-35 program. "To our knowledge, there has never been any classified information breach," the statement said. The Journal story didn’t say the stolen information was classified.

President Barack Obama, when he was a candidate for the White House, pledged to elevate cybersecurity as a national-security issue, equating it in significance with nuclear and biological weapons. A White House team reviewing cybersecurity policy has completed its recommendations, including the creation of a top White House cyberpolicy official. Details of that and other proposals are still under debate. A final decision from the president is expected soon.

A draft of the White House review steps gingerly around the question of how to improve computer security in the private sector, especially key infrastructure such as telecommunications and the electricity grid. The document stresses the importance of working with the private sector and civil-liberties groups to craft a solution, but doesn’t call for a specific government role, according to a person familiar with the draft.

Defense Secretary Robert Gates plans to announce the creation of a new military "cyber command" after the rollout of the White House review, according to military officials familiar with the plan.

The Pentagon has several command organizations structured according to both geography and operational responsibility. Central Command, for example, oversees the wars in Iraq and Afghanistan, while the Special Operations Command is responsible for operations involving elite operatives such as Navy Seals.
The cyber command is likely to be led by a military official of four-star rank, according to officials familiar with the proposal. It would, at least initially, be part of the Pentagon’s Strategic Command, which is currently responsible for computer-network security and other missions.

Pentagon officials said the front-runner to lead the new command is National Security Agency Director Keith Alexander, a three-star Army general. In a rare public appearance Tuesday at a cybersecurity conference in San Francisco, Gen. Alexander called for a “team” approach to cybersecurity that would give the NSA lead responsibility for protecting military and intelligence networks while the Department of Homeland Security worked to protect other government networks. His spokeswoman said he had no additional comment.

Former President George W. Bush’s top intelligence adviser, Mike McConnell, first proposed the creation of a unified cyber command last fall. The military’s cybersecurity efforts are currently divided between entities like the NSA and the Defense Information Systems Agency, which is responsible for ensuring secure and reliable communications for the military. The Air Force also runs a significant cybersecurity effort.

Advocates believe the new command will be able to avoid duplication and better leverage the technical expertise of the agencies and the military services’ cyberwarriors.

Cyber defense is the Department of Homeland Security’s responsibility, so the command would be charged with assisting that department’s defense efforts. The relationship would be similar to the way Northern Command supports Homeland Security with rescue capabilities in natural disasters. The NSA, where much of the government’s cybersecurity expertise is housed, established a similar relationship with Homeland Security through a cybersecurity initiative that the Bush administration began in its final year.

NSA’s increasingly muscular role in domestic cybersecurity has raised alarms among some officials and on Capitol Hill. Rod Beckstrom, former chief of the National Cyber Security Center, which is charged with coordinating cybersecurity activities across the U.S. government, resigned last month after warning that the growing reliance on the NSA was a "bad strategy" that posed "threats to our democratic processes."

Gen. Alexander countered in his speech Tuesday that the NSA did "not want to run cybersecurity for the U.S. government."

—August Cole contributed to this article.

Write to Siobhan Gorman at siobhan.gorman@wsj.com and Yochi J. Dreazen at yochi.dreazen@wsj.com