More than just information-sharing is needed, Dempsey and Alexander said. Key to addressing the threat is the adoption of minimum security requirements

WASHINGTON (AP) -- The Senate could leave town this week for a monthlong break without passing legislation to protect the U.S. electrical grid, water supplies and other critical industries from cyberattack and electronic espionage.

Congressional sponsors of the bill scrambled Wednesday to overcome Republican resistance to the measure, but they appeared short of the votes needed for passage despite dire warnings from top national security officials about the potential for devastating assaults on the computer networks that control the country's essential infrastructure.

President Barack Obama urged lawmakers to pass the legislation as soon as possible.

"He strongly, strongly believes that this nation's well-being is at risk from cyberattacks and intrusions," John Brennan, the president's assistant for homeland security and counterterrorism, said. "We find it hard to believe there is any reason or basis to oppose this legislation."

The principal stumbling block on Capitol Hill is what role the government should play in protecting U.S. businesses from cyberattacks. Republicans have argued that the bill would lead to mandatory rules imposed by Washington that would only increase the private sector's costs without substantially reducing the risks.

Senate Majority Leader Harry Reid, D-Nev., said major changes were made to the legislation to accommodate Republican concerns, and he accused the GOP of playing politics with a pressing national security issue. Instead of a thoughtful debate on the risks of cyberattacks, Reid said Wednesday, Republican senators have sought to offer unrelated amendments to the bill, including one to repeal Obama's health care law.

"I thought they were going to be serious about this," Reid said. "But they're not."

Senators are scheduled to vote Thursday on Reid's motion to limit debate and force a vote on the bill. But a super majority of 60 votes in the 100-member Senate is required to pass the motion, and Democrats only have 51, plus two independents who generally vote with the party. Sen. Susan Collins, a Republican from Maine and one of the bill's primary co-sponsors, will support the measure, but that leaves Reid six votes short.

Congress is scheduled to go on its August recess at the end of the week and won't return until after Labor Day.

Failure to approve the Senate's Cybersecurity Act of 2012 would amount to a rejection of the advice from senior national security officials, including Gen. Martin Dempsey, the chairman of the Joint Chiefs of Staff, who have been calling for Congress to act now on comprehensive legislation to deal with cyberthreats.

"The uncomfortable reality of our world today is that bits and bytes can be as threatening as bullets and bombs," Dempsey said in a letter Wednesday to Sen. Jay Rockefeller, D-W.Va.

The owners and operators of critical industries reported nearly 200 cyber intrusions in 2011, a nearly 400 percent increase from 2010, according to Collins and Sen. Joe Lieberman, I-Conn.,

who is one of the Cybersecurity Act's main authors. U.S. companies lose about $250 billion a year due to theft in cyberspace of intellectual property, Collins and Lieberman said.

Attackers are also becoming more aggressive, moving from the theft of data to the disruption of networks, said Army Gen. Keith Alexander, the top officer at the Pentagon's Cyber Command. "Our concern is that they're going toward destruction, which would have significant impact," Alexander said.

The Cybersecurity Act would create a framework for federal agencies and the private sector to share information about cyberthreats or malicious software that can destroy computer networks if it's not detected. Lieberman and Collins have said they have included provisions to ensure privacy and civil liberties aren't violated.

The most significant revision made to the legislation was the removal of a regulatory section, opposed by Republicans, that would have required companies operating critical infrastructure to meet basic cybersecurity standards established by the Homeland Security Department. The new version of the bill offered incentives, such as liability protection and technical assistance, to businesses that voluntarily participated in a government-managed cybersecurity program. Industry associations and groups would be involved in developing the standards needed to blunt the risks of cyberattacks, according to the revised legislation.

The U.S. Chamber of Commerce, which has been an influential voice during the debate, said the voluntary program was nothing more than a "springboard" to federal regulations that would take time and money away from efforts businesses already have under way to protect their networks. Once a "government-driven `voluntary' standards system is enacted," the Chamber said on its FreeEnterprise blog, "it's only a short hop to a mandatory one because the administration has the intent and regulatory leverage."

The Chamber is backing legislation drafted by Sen. John McCain, R-Ariz., similar to legislation passed by the House in late April. But those bills are focused on the sharing of threat information between the federal government and private sector. The White House threatened to veto the House bill, however, over concerns the bill didn't do enough to protect privacy rights.

More than just information-sharing is needed, Dempsey and Alexander said. Key to addressing

the threat is the adoption of minimum security requirements that would harden critical infrastructure networks and make it more difficult to conduct successful cyberattack penetration, they said.

"Minimum standards will help ensure there is no weak link in our infrastructure," Dempsey wrote in his letter to Rockefeller.