WASHINGTON — Nearly all the utilities that participated in two-day exercise last November to test the preparedness of the power grid for online and physical attacks said that their planning was not good enough, according to a report by the North American Electric Reliability Corporation, which organized the drill.

But the participants, more than 2,000 of them from across the United States, Canada and Mexico, said the exercise taught them lessons about whom they would need to communicate with in an attack, and where their vulnerabilities were.

The report had few details, because organizers said they did not want to provide a road map about the shortcomings and because they had promised to limit the scope of their evaluation to induce utilities to participate. But the reliability group is communicating with the utilities individually about their performances.

The drill provided “a one-two punch between cyber and physical security avenues,” said Bill Lawrence, manager of critical infrastructure protection awareness at the electric reliability corporation, which is charged by the government with enforcing standards of conduct on the grid.

It also uncovered more ordinary problems. For example, planners stress conference calls to keep all participants informed about attacks on their neighbors, but the conference system did not have enough telephone lines.

In the drill, participants spent a morning simulating 12 hours of attacks, then completed another 12 hours in the afternoon. On the second day, industry
executives and government officials conducted a “tabletop exercise” to explore when the federal government might step in during a coordinated attack.

The drill was called Gridex II, short for Grid Exercise. It was more than twice the size of the first one two years ago and participation exceeded the organizers’ expectations, reflecting wider anxiety about the grid as a vulnerable national asset. Another exercise is planned for 2015.

In the months since the drill, a report of an attack on a substation in California has raised more concern about vulnerability. Subsequent investigation by the police cast doubt on the idea that the attack was the work of more than one person with insider knowledge. But the Federal Energy Regulatory Commission has told the utilities to prepare reports about their vulnerabilities.

One issue is the security of the reports themselves, which would be a guide for an attacker.

The president of the reliability group, Gerry Cauley, said that establishing protection against attacks would have to be fit into context. Utilities are hardening their systems against big storms like Hurricane Sandy, he said, and are working on determining their vulnerability to solar activity that changes the earth’s magnetic field.

“We have to keep this always in perspective,” he said. The question was “getting the bang from the buck” spent on behalf of electricity customers for protection and resiliency. “We have to be always conscious of that balance,” he said.

Among the findings after the drill were that the utility system needed better access to additional transformers, which are large, hard to move and require long lead times for procurement. The California attack was on transformers. Also, utilities and law enforcement personnel need to “develop mechanisms to preserve evidence and collect forensic data following a suspected physical or cyberattack,” all while trying to get the lights back on. In the drill, emergency medical workers at the scene of a hypothetical attack were sometimes fired upon by the attackers.

The public report did not detail what the utilities said they had found lacking in their own planning. But it said that more than 98 percent found the exercise “useful for identifying opportunities to enhance their cyberincident response plans,” and 92 percent said the same for physical incident response plans.