From: Cherry, Brian K
Sent: 7/9/2013 3:46:37 PM
To: Liza Malashenko (elizaveta.malashenko@cpuc.ca.gov); Jack Hagan (Jack.Hagan@cpuc.ca.gov)
Cc:
Bcc:
Subject: Fwd: fyi - more on Metcalfe

FYI.

Brian K. Cherry
PG&E Company
VP, Regulatory Relations
77 Beale Street
San Francisco, CA. 94105
(415) 973-4977

Begin forwarded message:

From: "Bird, Katherine R" <KRBf@pge.com>
Date: July 9, 2013, 3:43:38 PM PDT
To: "Bottorff, Thomas E" <TEB3@pge.com>, "Hapner, Dede" <DxH4@pge.com>, "Cherry, Brian K" <BKC7@pge.com>, "Horner, Trina" <TNHc@pge.com>
Cc: "Allen, Meredith" <MEAe@pge.com>
Subject: fyi - more on Metcalfe

Fyi

NERC mulling options in light of recent shooting of Calif. substation, CEO says

Article

Related Content

To receive real-time alerts for stories on similar topics, click here.

By Esther Whieldon

The North American Electric Reliability Corp. has not decided whether there should be new standards to protect transmission assets from coordinated physical attacks following an incident in April in which someone riddled a bank of transformers at Pacific Gas and Electric Co.'s Metcalf substation near San Jose, Calif., with bullets from a high-powered rifle, NERC President and CEO Gerry Cauley said July 9.

FERC Chairman Jon Wellinghoff broached the question during a FERC conference on reliability (AD13-6) in Washington. Regarding the risk of a coordinated physical attack on transmission assets, what is NERC's role, "especially in light of Metcalf?" Wellinghoff asked. "What we can do here in the immediate future?"

"Like you, I've been concerned about it" for several years, and raised those concerns, Cauley said. "The challenge is sort of galvanizing action when we haven't seen any sort of major events," he said after giving a prepared statement.

NERC put out a best practices guide following the Sept. 11, 2001, terrorist attacks, Cauley said. "Once we saw the event at Metcalf, we issued an alert to try to raise awareness of industry in the near term." NERC has also asked "our technical experts" to review the physical security guidelines to make sure they are up to date, he said.

"The question really for me … is how do we ensure the accountability and appropriate action? It's a tough call because there are so many physical assets spread over such diverse areas," Cauley said. That said, he added, more needs to be done. "I think we, at least, have to encourage industry to take a look at the most critical high-priority assets and make sure that there are some sort of operational protections around those," Cauley said.

The "threshold question for me," said Wellinghoff, is whether protections from physical threats are "amenable to the standards process."

"I'm not sure I've landed on a firm conclusion at this point," Cauley said. "I think it's going to have to take some dialogue with industry in terms of what can be done cost effectively."

From the utility industry perspective, "I don't know that it's amendable to a standard that would apply to everyone," said Consolidated Edison Inc. CEO Kevin Burke, who represented the Edison Electric Institute at the FERC conference. "I think the best practices that NERC has put out and that we've been working with other utilities on [are] probably the better way to go."

Along those lines, FERC Commissioner John Norris asked the morning panel to describe the extent to which standards can address cybersecurity vulnerabilities.

"I think it's important that we move ahead with Version 5" of the critical infrastructure protection, or CIP, standards and implement them, Burke said. "I think the standards have to set a standard that we know everybody is abiding by."

That said, more may need to be done in some places such as "New York City, which could be more vulnerable to a cyberattack … simply because of the publicity you'd get if you could have an impact" on the city and economy, he said. "So we've continued to take some additional steps," such as meeting with agencies, "to try to continue to build the relationships and find out what they know. … And we have people in now just evaluating our computer systems."

Burke said those activities have reduced many of the company's cybersecurity risks. But he does not "know if you could do that with standards that would then apply to every utility in the country."

Cauley suggested that "we have to set the right expectation for what the standards would do and that would be to provide a baseline." People should not expect the CIP standards to "cure the cybersecurity threat" or that new standards would make it better, he said. "CIP 5 is going to hold us for a while."

However, NERC is taking steps outside of the standards process to deal with the dynamic nature of cyberthreats, Cauley said. For example, it is holding a drill in November with more than 100 companies to see how they would handle a major cyberattack, Cauley said.

Allen Mosher, the American Public Power Association's vice president of policy analysis and reliability standards, agreed with Cauley that NERC is done "for now" with updating its cybersecurity standards. The standards have gone through multiple iterations since they were first approved by FERC in 2008. A number of trade groups recently urged FERC not to mandate any changes to the Version 5 standards because any more directives would further complicate implementation.

"There's so much else that we need to do on cybersecurity," including collaboration with agencies and drills to see how the industry would recover from an attack, said Mosher, who formerly chaired the NERC standards committee. "We need to drill those things out through exercises so that when those actions happen we're not looking through a phone book for the person to contact" and so that companies are not inundated with calls from multiple people, Mosher said.