In This Section

- Public Power Daily
- Public Power Weekly
- Public Power Magazine
- Annual Directory & Statistical Report
- APPA's People to People
- Quarterly Communicator
- Washington Report

Public POWER

September 2008

:View Archived Issues:

Broadband

CALEA Compliance: Avoiding a $10,000 Fine

By: Cathy Swirbul

Broadband providers offering voice over Internet protocol services face a $10,000-a-day fine if they fail to comply with federal law requiring telecommunications providers to help law enforcement agencies.

Thirteen years after adoption of the Communications Assistance for Law Enforcement Act of 1994 (CALEA), the Federal Communications Commission and the courts expanded its scope to require voice over Internet protocol providers to acquire the technical capabilities to assist law enforcement. With the extension of these responsibilities, law enforcement can turn to VoIP providers for help when conducting authorized interceptions of communications content or to obtain call-identifying information. Under the law, providers had to become compliant by May 14, 2007.

“As the Federal Communications Commission has interpreted it, CALEA apparently applies to any provider of telecommunications or Internet services that could conceivably assist in surveillance, including the smallest municipality,” said Casey Lide, an attorney with the Baller Herbst Law Group, a firm that has worked with municipal broadband providers to help them become compliant with CALEA.

“Transmission is key,” Lide said. “If the service provider owns or controls facilities involved in the transmission of communications, it will likely be subject to CALEA, regardless of whether it possesses detailed information about the end-user customer.”

CALEA does not affect surveillance authority. A surveillance order must still be legally valid. “If a municipality were to get a subpoena or a request for a wiretap from law enforcement, it would still have to be sure that the request is legally sufficient under something other than CALEA,” said Jim Baller, president of Baller Herbst. “Our firm has created a manual on privacy for APPA members on what makes a law enforcement request legal.”

Many public power utilities have taken the steps necessary to comply with CALEA, Baller said. “There could conceivably be some entities, though, that are not yet in full compliance with CALEA.”

While CALEA’s scope is determined by the term “telecommunications carrier,” the meaning of that term, under

the law, is significantly broader than its use in other areas of telecommunications law. For CALEA, a telecommunications carrier includes broadband Internet access providers and interconnected voice over Internet protocol. Communications services offered through wireline, satellite, cable modem, wireless, fixed wireless and broadband over powerline may all be subject to CALEA.

Tthe complexities of Internet technology compared with traditional telephony contributed to the long delay in implementing a firm deadline for CALEA compliance, Baller said. “With traditional circuit-switched telephony, you can easily find a good point along the transmission path to tap into a call. In contrast, in the IP world, calls are often broken into small ‘packets,’ and these packets find their way over separate paths around the world to the destination, where they are re-assembled. As a result, in some cases, no single entity may have access to an entire message,” Baller said. “The Federal Communications Commission, the Department of Justice, and the industry took a long time to work out these complexities, create standards, and determine to whom they would apply.”

“As the world moves telephone communications to the Internet, the targets of investigations are migrating to broadband communications, and law enforcement officials must be able to keep up with them.” Baller said. “Reading CALEA as exempting broadband communications would have created significant problems for law enforcement, so the Federal Communications Commission and the courts stretched the language of the act to find broad coverage.”

At the end of 2006, Baller Herbst, partnering with Columbia Telecommunications Corp., joined forces with about 25 public power utilities to address the intricacies of CALEA and assist them with deciding what would work best for each provider when filing with the Federal Communications Commission. Some larger municipal utilities and a few with special expertise are implementing the compliance technology themselves, Baller said. Others are outsourcing tasks to third parties. Since the collaborative formed, CALEA compliance technologies and business models have evolved, adding to the compliance options available.

Whether a municipality works in-house or hires a third party, the compliance process is similar: surveying the existing infrastructure; determining the possible number of simultaneous intercepts; designing a configuration for the provider’s particular architecture; perhaps, installing a mediation device and/or a CALEA administrative device; and, possibly, upgrading network switches and the network software.

Some municipalities had initial concerns about entrusting a third party with confidential customer information, said Baller.

“Privacy issues should be dealt with up-front in hiring a third party, when all the initial documents are being signed,” Lide said. “Some technical approaches would shunt all the communications traffic to a remote third party, who would then pick out the information law enforcement is requesting. The third party probably is acting as the municipal’s agent in these cases, but the legal relationship needs to be carefully considered.”

Another compliance option is known as “just-in-time,” when a provider does essentially nothing until it receives a surveillance request. “This could be a somewhat risky approach,” Lide said. “A provider might be unable to comply in time to satisfy CALEA’s assistance capability requirements.”

“There is also a very real question whether the just-in-time option could be implemented fast enough to satisfy law enforcement officials, particularly in time-critical situations.” Lide said. “As the FCC explained to us, ‘when planes are crashing into buildings, law enforcement officials are going to want immediate access to critical information, and they’re not going to be sympathetic to entities covered by CALEA that can’t provide it immediately.’”

The cost of compliance will depend largely on what hardware and software a provider currently has in place, and the size of the provider’s subscriber base. Some compliance providers require a comparatively small amount of money up front, with more required in the event of an interception request. Others charge most of the fee up front. Some charge a monthly subscription fee.

“There are a variety of technological and financial options,” Lide said. “That’s why we brought Columbia Telecommunications into the process. They can handle the design, engineering, technology, and cost issues.”

Providers of telecommunications service, Internet access, and interconnected voice over Internet protocol must be sure they understand their responsibilities and do what’s necessary to meet them, said Baller.

<< Back to Public Power Magazine Listing

Digital Edition | 2009 Media Guide | 2008 Media Guide | Ad Insertion Order | Reprints | Reader Comments | E-mail the Editor
View Archived Issues

Back to Top

American Public Power Association 1875 Connecticut Ave. NW, Suite 1200, Washington, DC 20009-5715
Tel: 202.467.2900 Fax: 202.467.2910 Copyright Privacy Policy