

CALEA COMPLIANCE SERVICE FOR BROADBAND SERVICE PROVIDERS

In May of 2006, the Federal Communications Commission (FCC) issued a second order extending the Communications Assistance for Law Enforcement Act (CALEA) to providers of broadband Internet access and interconnected voice-over-IP (VoIP) services. The U.S. Court of Appeals for the D.C. Circuit recently upheld that order on appeal. As a result of this ruling, broadband service providers must be in compliance with CALEA's provisions by May 14th, 2007.

Background

The Communications Assistance for Law Enforcement Act was passed in 1994 to enable the FCC to compel carriers to provide better assistance to law enforcement in carrying out wiretaps in the newer digital PSTN infrastructure. In 2004, the FCC proposed rule changes that would take into consideration newer Internet communications capabilities (packet based technologies) such as VoIP. Law enforcement's concern was that they would be required to master new technologies each time they issued a wiretap warrant. As the FBI and local police don't have the resources to be technology experts for every new communications medium, they sought the FCC's help in compelling broadband Internet service providers (ISP) and interconnected VoIP providers to provide an on-demand capability to enable electronic surveillance of their clients if presented with a warrant. The FCC agreed and expanded CALEA provisions to broadband ISP's and VoIP providers, setting a March 14th, 2007 deadline for compliance with the law. This means all broadband ISP's must augment existing equipment or add an intermediary device to transparently intercept only the traffic allowed by a warrant. In addition, each ISP will need to file documentation with the FCC certifying their compliance (via FCC Form 445) by February 12th, 2007 and file a System Security and Integrity (SSI) plan by March 12th, 2007.

Challenge

Deploying a transparent intercept solution into your infrastructure can be a daunting task. There are a multitude of costly solutions on the market designed for large common carrier and VoIP providers. These solutions don't scale well, from a cost or sizing perspective, into most broadband service provider networks. Other concerns include: What constitutes compliance? How do I know that our intercept solution will meet law enforcement's needs? Will our output be legally admissible in a court of law? Will my clients' privacy be protected? How do I avoid the negative public relations consequences of a privacy breach?



BEARHILL SECURITY

BearHill Security, Inc.
395 Totten Pond Road
Suite 303
Waltham, MA 02451

Phone: 800-618-4487
Fax: 781-487-5779
Web: www.bearhill.com

Simplifying Security

Solution

BearHill is a Trusted Third Party provider (TTP) of CALEA compliance services and offers a managed CALEA solution. Over the past several years BearHill has developed a deep repertoire of forensic investigation expertise through our information security consultancy. Additionally, we were able to leverage our secure operations platform designed to support our Ensure intrusion prevention service. By combining our forensic investigation expertise with our existing secure operations platform, BearHill is able to offer broadband ISPs a cost effective intercept access service that meets FCC and law enforcement requirements.

BearHill's CALEA compliance service is a comprehensive solution that incorporates planning and design, a passive intermediary intercept access appliance, 24 x 7 warrant execution support, and a process and procedure plan. The CALEA compliance service includes the following features and benefits:

BearTrap IAP – the BearTrap Intercept Access Point (IAP) is a purpose built, hardened platform designed to provide passive data intercept capabilities. The BearTrap provides target specific data intercept capabilities and enables the service provider to fulfill warrant requests with a standardized data output that satisfies law enforcement requirements.

Passive Network Presence – The BearTrap IAP is a passive device that doesn't add latency or a point of failure to your infrastructure and enables transparent data capture as required by CALEA.

Design and Implementation Assistance – BearHill's security architects will assist you in determining the optimal location to deploy the BearTrap IAP and ensure its security.

Policy and Procedure Planning – BearHill will assist your team in creating detailed policies and procedures that will ensure your management retains control over the data intercept process. The final plan can be filed with the FCC to satisfy the System Security and Integrity Plan documentation requirement.

24 x 7 x 365 Support Team – BearHill's team is available to execute warrant requests upon authorization of the service provider's management team. Further, BearHill continuously monitors the BearTrap to validate that the service provider is capable of meeting CALEA's requirement to provide on-demand intercept capabilities.

About BearHill

BearHill Security provides information security consulting, network forensics, network security services and investigative expertise to a wide range of companies, state and local governments, Federal and state agencies, and law enforcement organizations worldwide. Fortune 500® Companies rely on BearHill to safeguard their reputations and to insure continuity of their business operations.

BearHill's strengths are derived from the expertise of an exceptional technical team that has a singular focus: information security. Our team members have diverse backgrounds that range from designing and implementing critical government communications systems, such as the White House Situation Room, to securing the assets of multinational financial investment banking and securities firms. BearHill team members possess a variety of information security and networking certifications, and collectively have many years of relevant experience in the network, system administration, and security fields. In addition, BearHill team members undergo extensive background investigations and possess U.S. Government Security Clearances. This combination of experience and specialized focus provides an ideal source of collaboration and peer review for our clientele and aids in the creation of technically sound and secure environments.