

CALEA Compliance & Lawful Intercept

Gigamon Aggregation for CALEA Compliance and Lawful Intercept

CALEA Compliance

- **What is CALEA?**
- **Does CALEA affect me?**
- **What should I know about CALEA?**
- **Are there any lessons that I can learn from CALEA Compliance that would help me better manage my enterprise network?**

CALEA is an acronym for Communications Assistance for Law Enforcement Act, originally enacted in 1984 by the U.S. Congress.

This law as previously drafted was focused only on the monitoring and capturing requirements for telecommunication carriers and service providers when mandated through court orders or other lawful authorizations.

As of May 2006, the law has been broadly extended to include all VoIP carriers forcing many smaller non-traditional providers to comply with the same access and capture parameters.

There is even serious talk about removing the exemption for both public and private Universities and requiring them to come into compliance in the near future.

Interestingly, CALEA is also the name of a plant that is alleged to be capable of “clarifying the senses”, which the Chontal medicine men call *thle-pela-kano*, meaning “Leaf of God”. According to Wikipedia, [Calea Zacatechichi](#), also known as Dream Herb, Cheech, and Bitter Grass, is still used by the indigenous Chontal of the Mexican state of Oaxaca for oneiromancy, which is a form of divination based on dreams. Whenever they desire to investigate the cause of an illness or the location of a lost or distant relative, dry leaves of the plant are smoked, drunk in infusions, and put under the pillow before going to sleep, expecting the answer to the difficult question to materialize in a dream.

CALEA Compliance is the “Bitter Grass” of our time. While painful to implement, once successfully deployed, CALEA compliance tools can actually provide us with previously unavailable visibility to our own network, allowing us to “clarify our senses”.

Often you hear the phrase “Lawful Intercept” as a definition of CALEA such that any enactment resulting from a warrant or court order would be a “Lawful Intercept”. However, Lawful Intercept has a much broader spectrum of applicability than CALEA. I prefer to use the term “Lawful Monitoring” since it extends to anyone who has authority under the law to support monitoring in order to prevent misuse of networks, which extend beyond telecom to include enterprises and educational networks and facilities.

CALEA Compliance & Lawful Intercept

“Lawful Monitoring” involves network managers and technicians who as part of their ongoing support of a network have lawful access to monitor, record, analyze and report on network activities and user behavior. Increasingly, managers and technicians are subpoenaed as witnesses to testify against aberrant behaviors including abuse of corporate policies and/or potential violation of the laws of the land – municipal, city, county, state, federal and even international; such actions could be the result of a lawsuit or even part of a Freedom of Information inquiry.

What should I know about CALEA?

Basically CALEA requires that traffic access points (TAP's) be installed throughout the network, giving FULL ACCESS to every packet traversed within the production network. When a warrant is issued, this access device would be connected to the warrant device, which would be configured to capture the IP address specified or other traffic variables required within the authority of the warrant. Once the time or event prescribed in the warrant has occurred, the data (evidence) is gathered and stored in a transferable medium or routed through a third party network to the requesting agency, with appropriate time stamping, etc.

Trusted Third Parties like Apogee Intercept Service and SS8 are companies that install access points and their special recording device for either a set cost or monthly fee, or both. When a warrant is issued, the Trusted Third Party configures their router device to forward the specified traffic to either a remote capture device or to the requesting agency directly. Associated fees charged by Trusted Third Parties to execute the warrant(s) can add up quickly, so one needs to have a complete and thorough understanding of the cost structure before engaging third party providers.

Are there any lessons that I can learn from CALEA compliance that would help me better manage my enterprise network?

If customers do not wish to relinquish control of their network to third parties, which is almost always the case, they need to deploy CALEA solution and access taps directly and handle all warrant activities on their own. The following shows a typical CALEA compliance tool set which involves three interoperating components: 1) a number of passive taps (e.g., [Gigamon](#)), 2) if the network is complex enough, an aggregation and data access switch (e.g., [Gigamon](#)) and 3) a line-rate packet capture forensics recorder with off-line storage capability (e.g., [Solera Networks](#)).

In addition to substantial cost saving, deploying your own CALEA compliance tools can be a very valuable investment for network managers since each of these components can bring tremendous benefits in normal network operations:

1. To be able to do their job as network managers, they need to have full access to their network at anytime from anywhere for any and all types of monitoring, analysis, etc. Obviously, once a network is deemed CALEA compliant, it is essentially fully instrumented. Taps installed for the purpose of CALEA

CALEA Compliance & Lawful Intercept

- compliance can be used to gain unobtrusive and high fidelity access to the production traffic. These taps can be used in collaboration with the SPAN ports that are already available on the switches.
2. Once their network is CALEA compliant, as network managers, they have in their tool arsenal a powerful packet capture engine with sufficient storage capacity so that they constantly have a few days worth of stored data to review issues and anomalies that have occurred while they were not watching the network. Capturing all packets is a necessity for complete forensic analysis.
 3. Most CALEA compliant solution provides the ability to aggregate traffic from multiple taps and perform hardware packet filtering in order to focus the investigation on certain logical attributes, application type, IP address, VLAN, etc. This capability would be a value-add to the network managers since they now have the means to perform focused troubleshooting and performance review.

CALEA Compliance is a bitter medicine.

Even though enterprise managers are not currently required to be CALEA compliant, it is in every manager's best interest to learn from the best practice CALEA compliance solution to define and support their internal policies and procedures.

Managers should take full advantage of any ability to have 100% access to their data with taps correctly placed in their network, capturing all the data or filtering (pre or post capture) the data so they can perform forensics review for a period that is longer than a few days. Whatever platform they choose for packet-capture should be very flexible and have the ability to expand as the network and support requirements grow.

CALEA & Lawful Intercept

- Forensics & Data Capture
- Out-of-Band Data Access

Finally, when purchasing a CALEA Compliance product or solution, keep in mind the following:

- The product should fit your needs today in supporting your network, i.e., defining network policies, enforcing current corporate policies, troubleshooting and analysis requirements.
- Always purchase a solution that is as open to many other applications as possible, from Open Source to Proprietary
- Buy a solution that is compatible with your current legacy monitoring, analysis, reporting and other applications. (Do not get caught up buying an all-proprietary technology unless you are sure that it is exactly what you need.)
- Always purchase a solution that can be upgraded easily and at a reasonable cost. If possible purchase a solution that you have tried in your network and have very good references for.

CALEA Compliance & Lawful Intercept

Summary

CALEA is only one of many compliance standards facing businesses today. They will soon spread to all areas of networking, so be prepared and be proactive! Adopting a CALEA mindset to supporting one's network will definitely pay off.

About Gigamon

Gigamon delivers intelligent data access solutions to enhance monitoring of service provider and enterprise data centers. The company's world-renowned GigaVUE™ "orange boxes" aggregate, filter and replicate customized data streams to all monitoring tools. Gigamon pioneered technology for multi-tool environments to address new demands for reporting and analyzing organizational data. Now in its third generation with global deployments in over 40 countries and 90 percent market share for intelligent data access, Gigamon's GigaVUE platform is the only proven, fully-integrated, total solution for all data access needs. Gigamon's patented technology enables companies to realize day one ROI by increasing tool value and operational efficiencies. GigaVUE ensures seamless and controlled delivery of the right data, at the right time to the right tools. Organizations deploying Gigamon solutions enjoy greater uptime, reduced threat vulnerability and improved regulatory compliance. For more information about Gigamon and its award-winning solutions, visit www.gigamon.com

Author: Tim O'Neill The "Oldcommguy"

Media Contact:

Grant Swanson

Marketing Manager

Gigamon

grant.swanson@gigamon.com