

**Before the  
Federal Communications Commission  
Washington, D.C. 20554**

In the Matter of	)	
	)	
Communications Assistance for Law	)	ET Docket No. 04-295
Enforcement Act and Broadband Access	)	
Services	)	RM-10865
	)	

**Opposition of VeriSign, Inc.**

**United States Telecom Association Petition for Reconsideration  
and for Clarification of the *CALEA Applicability Order***

Anthony M. Rutkowski  
Vice President for Regulatory Affairs  
VeriSign Communications Services Div.  
21355 Ridgetop Circle  
Dulles VA 20166-6503  
tel: +1 703.948.4305  
mailto:trutkowski@verisign.com

Peter Wiederspan  
Director, NetDiscovery Service  
4501 Intelco Loop SE  
Olympia, WA 98503  
tel: +1 360.493.6220  
mailto:pwiederspan@verisign.com

Michael Aisenberg  
Director, Government Relations  
1666 K Street, N.W., Suite 410  
Washington DC 20006-1227  
tel: +1 202.973.6611  
mailto:maisenberg@verisign.com

Brian Cute  
Director, Government Relations  
1666 K Street, N.W., Suite 410  
Washington DC 20006-1227  
tel: +1 202.973.6615  
mailto:bcute@verisign.com

Filed: 19 January 2006

1. On 5 August 2005, the Commission adopted its *First Order* in this proceeding.<sup>1</sup> On 14 November, the United States Telecom Association (USTA) filed with the Commission a *Petition for Reconsideration and for Clarification of the CALEA Applicability Order (USTA Petition)* in this proceeding, requesting that the Commission: 1) "...should reconsider its decision to start the 18-month clock on November 14, 2005....[i]nstead, the Commission should start that clock on the effective date of its forthcoming order on CALEA capability requirements for broadband and VoIP providers, and 2) "...spell out the specific broadband access services that are “newly covered services” subject to the 18-month compliance timetable.”<sup>2</sup> On 4 January 2006, notice of the petition was published in the Federal Register.<sup>3</sup> VeriSign, Inc., (VeriSign) opposes the first requested action in the *USTA Petition*. The second action seems unnecessary as the claimed lack of clarity is not apparent.

## **I. THE CALEA *FIRST ORDER* PROVIDES AMPLE DIRECTION AS TO WHAT AVAILABLE CAPABILITIES ARE REQUIRED BY BROADBAND AND VoIP PROVIDERS**

2. The thrust of USTA’s argument for a delay in the implementation of the 18 month CALEA implementation timeframe is an assertion that the Commission did not provide sufficient “answers to...basic questions about the scope of [broadband and VoIP providers] CALEA obligations.”<sup>4</sup> What the assertion ignores, however, is the several years of industry collaborative activity together with the FBI that has ensued to define those CALEA’s Sec. 103 capabilities for broadband and VoIP providers and turn them into detailed standards that have subsequently been implemented by vendors, service bureaus, and providers. There is no broadband or VoIP provider who cannot become fully compliant today – much less by 17 May 2007 – with the simple implementation of

---

<sup>1</sup> See *First Report and Order and Further Notice of Proposed Rulemaking* in the Matter of Communications Assistance for Law Enforcement Act and Broadband and Access Services in ET Docket No. 04-295, RM-10865, Doc. FCC 05-153, 20 FCC Rcd 14989 (23 Sept 2005) (“First Order”).

<sup>2</sup> *USTA Petition* at 3.

<sup>3</sup> See 71 Fed. Reg. 345.

<sup>4</sup> *USTA Petition* at 3.

readily available products or the procurement of a cost-effective CALEA third party service bureau offering.

3. The activity surrounding this proceeding began more than five years ago when the Internet Protocol (IP) started to be used significantly as a replacement protocol within the nation's public telecommunication network infrastructure, followed by the emergence of IP-based emulations of public network call signalling protocols and their introduction as commercial public services. As this technical and operational evolution began to unfold, the U.S. Department of Justice (USDOJ) and their counterparts worldwide began working closely with industry to assure needed forensic capabilities to assist law enforcement remained available – successfully progressing the work in multiple domestic and international workshops, conferences, requirements documents, and standards bodies. Especially noteworthy were two major workshops in 2003 - sponsored by the FBI to discuss the requirements with industry and make available two detailed requirements documents. Finally, in early 2004 after extensive industry collaboration to achieve the development of these capabilities, the USDOJ, FBI, and DEA jointly took steps to initiate the instant proceeding – aimed at providing a minimal, consistent, ubiquitous forensic “handover” capability in the public network infrastructure that was available to acquire evidence when authorized pursuant to law.

4. After 18 months and two commenting cycles in the instant proceeding that included more than 700 comments, the Commission's *First Order* was adopted - taking narrow and carefully determined steps to institute CALEA-based forensic capabilities that were not only developed within the industry together with law enforcement, but also started to become deployed in anticipation of the Commission's actions in this proceeding. Substantial investments have been made within the industry generally, and by VeriSign in particular, to achieve this compliance capacity for providers.

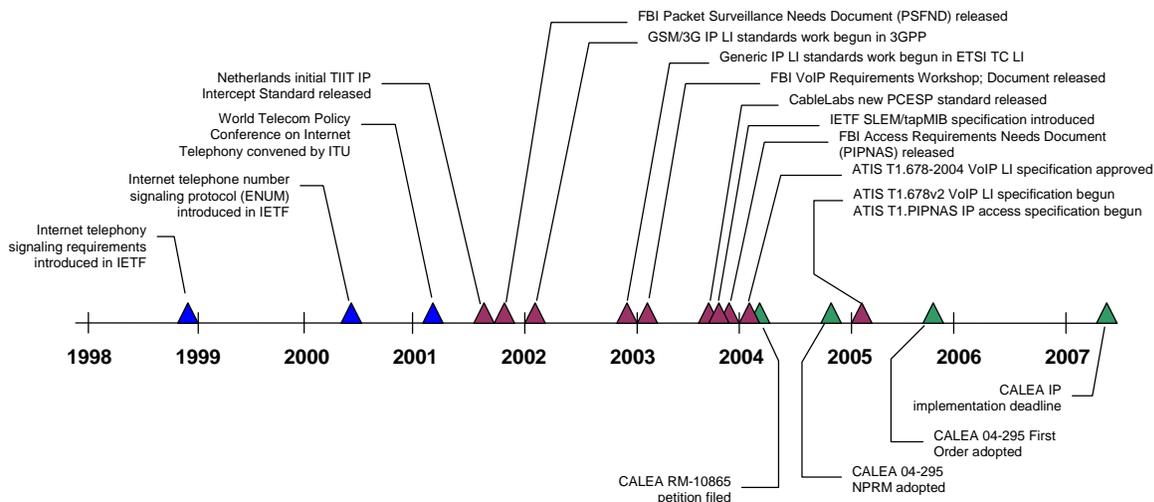


Fig. 1. IP-Enabled Public Communications Infrastructure - CALEA Continuum Timeline

5. USTA’s argument that the *First Order* requirements “lack any meaningful direction as to what those capabilities are supposed to be”<sup>5</sup> rings rather hollow against the history that has ensued over the past several years, and is not supportable in light of the facts. Figure 1, above, provides a general overview of the instant proceeding (green triangles) against the backdrop of infrastructure evolution (blue triangles) and industry - law enforcement collaborative activities (plum triangles). This extensive cooperation and consultation has ensued pursuant to Secs. 103, 104, 106 and 107 of the CALEA statutory provisions, exactly as Congress intended.<sup>6</sup> It has involved the work of hundreds of individuals and scores of companies working together over the past several years in more than a dozen different domestic and international industry standards forums to produce the necessary capabilities specifications required in the Commission’s *First Order*. This collaboration in turn has resulted in the communications and network forensics industries investing significantly in the development and deployment of equipment, software, and facilities in anticipation of Commission’s *First Order*. The requirements for full compliance with the *First Order* have been known for nearly three years, and the means of complying at low-cost with no adverse effects on technology are available today.

<sup>5</sup> USTA Petition at 2.

<sup>6</sup> See *Communications Assistance for Law Enforcement Act of 1994*, Pub. L. No. 103-414, 108 Stat. 4279.

Affected service providers have two readily available options: implement the requirements themselves or through available service bureaus.

**A. The Commission's 18 Month Deadline Is Compatible with Continuing Industry Developments**

6. The Commission's 18 month deadline for a digital forensics law enforcement support capability - imposed pursuant to either CALEA or Title I authority on facilities-based broadband Internet access providers and PSTN interconnected VoIP providers nearly 8 years after the technology first began to be standardized for introduction as part of the national public telecommunication infrastructure, four years after the release of the FCC's detailed requirements document, three years after commercial solutions appeared in the marketplace, and at a point where use of the technology is in U.S. households is projected to grow from 400,000 in 2004 to 12.1 million in 2009 - is neither arbitrary nor capricious.<sup>7</sup> The deadline seems well considered and highly appropriate in light of these trends. Indeed, exercising Title I authority, the Commission has adopted public safety E911 capability requirements within much shorter timeframes.<sup>8</sup> Whether the capability requirements are for public safety, preventing cyberstalking, forensic support for law enforcement, infrastructure protection, consumer protection, or national security/emergency preparedness, such actions are consistent with the Commission's authority accorded by Congress and affirmed by the Court.<sup>9</sup>

7. In light of the rapid transition of the public telecommunication infrastructure to IP-enabled systems and VoIP now underway, it would be especially inappropriate for the Commission to delay implementing the *First Order* CALEA requirements. See Fig. 2, below. At this point in the ongoing technological transition, it is relatively easy and inexpensive for vendors to include the required network forensic features in the new systems being built, and for service providers to implement the capabilities to meet

---

<sup>7</sup> See *Broadband Telephony: Leveraging Voice Over IP to Facilitate Competitive Voice Services*, Jupiter Research, Oct 2004. See also, Cybertelecom, VoIP Statistics <<http://www.cybertelecom.org/data/voip.htm>>

<sup>8</sup> See *First Report and Order and Notice of Proposed Rulemaking*, In the Matters of IP-Enabled Services (WC Docket No. 04-36) and E911 Requirements for IP-Enabled Service Providers (WC Docket No. 05-196), Doc. FCC 05-116, 3 June 2005.

<sup>9</sup> See *id.* at para. 4; *National Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 125 S. Ct. 2688 (2005) (hereinafter referred to as *Brand-X*).

CALEA mandates. The ensuing 18-month period is precisely when it makes good public policy sense to uniformly implement the capabilities. Furthermore, the mandated capabilities are generic, and not technology dependent. Delaying implementation of the CALEA capabilities would potentially result in more costly retrofitting of systems to become compliant at a later date

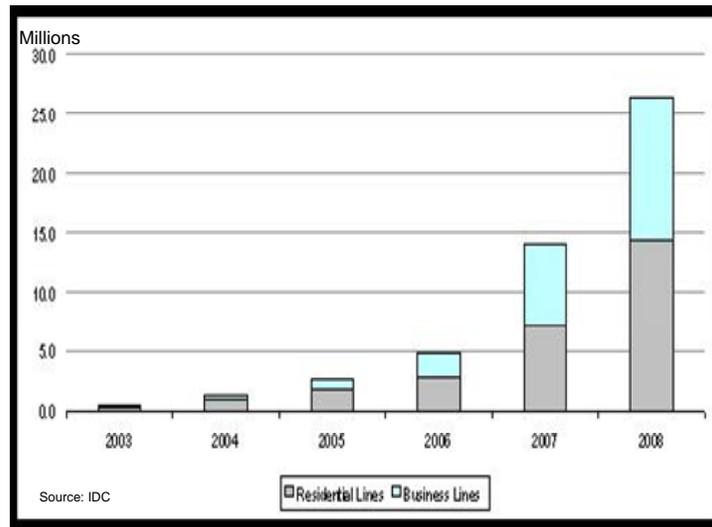


Fig. 2. Increase in North American VoIP Telephone Lines

**B. The Compliance Measures for VoIP and Internet Broadband Access, Including Covered Services, Have Long Been Well Known**

8. USTA’s argument for resetting the 18-month clock is based solely on their vague assertions about lack of any meaningful direction about the required capabilities. In fact, the Federal Bureau of Investigation (Bureau) initially made the requirements known more than four years ago.<sup>10</sup> The precise capabilities at issue here were explicitly conveyed to industry in 2003, and the Bureau conducted two day-long industry workshops at the time of the requirements release to help clarify these specifications and allow interaction with a broad array of industry attendees.<sup>11</sup> Several other widely

<sup>10</sup> See *Packet Surveillance Fundamental Needs Document (PSFND) for Telecommunications Carriers, Equipment Manufacturers, and Providers of Telecommunications Support Services*, Issue 1.0, October 31, 2001, CALEA Implementation Section, Federal Bureau of Investigation.

<sup>11</sup> See, e.g., *Electronic Surveillance Needs for Carrier-Grade Voice over Packet (CGVoP) Service*, Issue 1, January 29, 2003, CALEA Implementation Section, Federal Bureau of Investigation; *Surveillance for Voice over Packet Summit*, 23 Jan 2003 at Chicago; *Electronic Surveillance Needs for Public IP Network Access Service (PIPNAS)*, Issue 1, September 30, 2003, CALEA Implementation Section, Federal Bureau of Investigation; *LAES for Public IP Network Access Service (PIPNAS) Summit*, 2 Oct 2003 at Chicago.

attended industry workshops and other outreach initiatives were conducted by the Bureau's CALEA Implementation Section and Quantico Engineering Research Facility. The capability specifications were also provided upon request via the well-known CALEA Implementation Section website.<sup>12</sup> Over the subsequent years, scores of meetings and thousands of hours of productive work have ensued in domestic and international industry standards forums with active involvement of the Bureau and their contractors and virtually every sector of the telecommunications and network forensics industry. As a result, multiple standards have been produced to meet the capability requirements – which in turn have resulted in equipment being produced, capabilities tested, and services offered.<sup>13</sup>

**C. Trusted Third Party CALEA solutions have long been used for compliance**

9. Notwithstanding the Commission's reference in the *First Order* to existing satisfactory implementations of the capabilities at issue by VeriSign and other trusted third party service bureaus, USTA asserts that "...[t]he Commission did not...approve the use of trusted third parties, nor did it explain how a provider who uses a trusted third party could satisfy its CALEA obligations to safeguard the privacy and security of content and call-identifying information or its CALEA obligations to protect information about government's surveillance activities."<sup>14</sup> Here also, USTA ignores the fact that trusted third party service bureaus operate as a contractor agent for the provider, are accommodated in existing Commission CALEA provisions; and have been accepted by the FCC and law enforcement for the past four years.<sup>15</sup> As a contractor agent, such

---

<sup>12</sup> See [www.askcalea.com](http://www.askcalea.com), [www.askcalea.net](http://www.askcalea.net), [www.askcalea.org](http://www.askcalea.org).

<sup>13</sup> See, e.g., *PacketCable™ Electronic Surveillance Specification*, PKT-SP-ESP-I04-040723; Cable Labs, 23 Jul 2004; *Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks*, American National Standard for Telecommunications T1.678-2004; Draft, *Proposed for Lawfully Authorized Electronic Surveillance (LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks, Version 2*, ATIS-1000678.200X; *Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access*, ANS T1.IPNA-YEAR, Oct 2005; *Technical Specification, Universal Mobile Telecommunications System (UMTS), 3G security, Handover interface for Lawful Interception (LI)*, ETSI TS 133108 V6.9.0 (2005-06-27).

<sup>14</sup> See n.3, *supra*; USTA Petition at 2.

<sup>15</sup> 47 CFR § 64.2103 provides considerable latitude to the CALEA carrier that amply embrace the use of a Trusted Third Party. A telecommunications carrier shall:

service bureaus are subject to the same safeguard and protection requirements as the provider. Indeed, the layering, distributed nature, and interoperation of telecommunication infrastructure today inherently compel most CALEA carriers to rely on third party contractor agents supporting some CALEA related capability components today.

#### **IV. THE *USTA PETITION* SHOULD BE DENIED**

10. For all of the above reasons, the Commission should deny the *USTA Petition* with respect to any delay in the existing 18 month compliance deadline. A delay in the implementation deadline of another six to twelve months beyond the 18 months already established, denies law enforcement these capabilities and does potential harm to protection of the nation's public infrastructure. The required capabilities are critical not only to the investigation and prosecution of extrinsic crimes committed via communication networks, but also to detect and pursue those bent on committing criminal acts harmful to the infrastructure itself.<sup>16</sup> The Commission is acting here not only under CALEA authority, but also Title I responsibilities given to the Commission

- 
- (a) Appoint a senior officer or employee responsible for ensuring that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier.
  - (b) Establish policies and procedures to implement paragraph (a) of this section, to include:
    - (1) A statement that carrier personnel must receive appropriate legal authorization and appropriate carrier authorization before enabling law enforcement officials and carrier personnel to implement the interception of communications or access to call identifying information;
    - (2) An interpretation of the phrase "appropriate authorization" that encompasses the definitions of appropriate legal authorization and appropriate carrier authorization, as used in paragraph (b)(1) of this section;

A number of domestic and transnational submissions have been made to the Commission pursuant to 47 CFR § 64.2105 that rely on Trusted Third Parties. As long as a responsible senior officer or employee" of the carrier exists for purposes of meeting the 47 CFR § 64.2103 requirement, it is not apparent that any impediments exist, and no submissions have been declined by the Commission as insufficient on this basis.

<sup>16</sup> Indeed, USTA seems to acknowledge this concern in its treatment of its second subject of reconsideration, stating "requiring different timetables for compliance would also run counter to public policy by permitting individuals to avoid electronic surveillance simply by virtue of what broadband access service they choose." If it is against the public interest to adopted different timetables, it is certainly of greater concern to have the entire timetable delayed for everyone.

for protecting the nation's communication infrastructure, as well as the new *Prevent Cyberstalking* authority and mandate recently signed into law.<sup>17</sup>

---

<sup>17</sup> See H.R. 3402, *Violence Against Women and Department of Justice Reauthorization Act of 2005 (Enrolled as Agreed to or Passed by Both House and Senate)*, Public Law No. 109-162; President Signs H.R. 3402, the "Violence Against Women and Department of Justice Reauthorization Act of 2005," Office of the Press Secretary, The White House, Jan 5, 2006. See also, House Report 109-233 - Department of Justice Appropriations Authorization Act, Fiscal Years 2006 Through 2009.