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

In the Matter of	)	
	)	
Protecting Against National Security Threats to the	)	WC Docket Nos. 18-89
Communications Supply Chain Through FCC	)	
Rules and Regulation Implementing the Truth in	)	
Programs	)	

Comments of Yaana Technologies LLC

Anthony M. Rutkowski
EVP for Standards and Regulatory Affairs
Yaana Technologies LLC
542 Gibraltar Drive
Milpitas CA 95035
tel: +1 703.999.8270
mailto:tony@yaana.com

Filed: 26 Feb 2020

1. Yaana Technologies LLC (Yaana) requests the Commission accept these late filed comments by waiver to address one significant matter raised in the above captioned docket – the implementation of adopted CALEA 5G standards for Lawful Interception (LI) and Retained Data (RD).[1] If the waiver is not granted, these comments can be treated as *ex parte* information.

2. Yaana Technologies LLC (Yaana) is a Silicon Valley based global provider of security-related telecommunication and internet compliance obligation services. See www.yaanatech.com. For more than twenty years, Yaana and its senior staff have devoted significant resources to participation in LI/RD regulatory proceedings and industry technical standards activities and trade shows in the United States, multiple other nations, as well as regional and intergovernmental bodies – in many cases leading individual industry LI/RD standards work items. In the original CALEA Docket 04-295 proceeding, Yaana's NetDiscovery® services group[2] was also a prominent advocate for cost-effective solutions for USF supported providers, and devoting funds to meeting their CALEA obligations. During the past five years, Yaana has participated significantly in venues developing the 5G LI/RD requirements and standards at issue in this proceeding, and has itself developed and implemented the compliance solutions specified.

3. Yaana takes no position with respect to the treatment of individual 5G equipment suppliers in the Commission's exercise of its CALEA authority. However, with FCC assertion of CALEA jurisdiction, comes an obligation to uniformly apply the 5G LI/RD technical standards already adopted through industry-government collaboration, to all suppliers of equipment required to meet CALEA requirements. Those standards include many critically important requirements in addition to just supply chain management, and provide for compartmentalized LI capabilities plus other measures and architectures to reduce the risks and threats raised in Appendix E of the *Report & Order*. Not all 5G equipment must be CALEA capable, and overlay solutions are an option.

---

[1] Lawful Interception is the global term that is synonymous with the Lawfully Authorized Electronic Surveillance (LAES) capability used in Section 103 of CALEA, and used by almost all related industry standards bodies. Retained Data is the global term for access to non-LAES information under CALEA. The provision of 5G retained location data is known as Lawful Access Location Services (LALS). *See* ETSI TR 101567, *Lawful Interception (LI); Cloud/Virtual Services for Lawful Interception (LI) and Retained Data (RD*), 2016.

[2] The group in the proceeding was part of Verisign, Inc.

A. The Commission has jurisdiction and authority under CALEA to prescribe such rules as necessary to implement the requirements

4. At the time of enacting CALEA, Congress made it plain that the communication network environment was highly dynamic, and that continuing collaborative processes would be necessary among the FCC, the FBI and industry. Indeed, many of the dynamic changes in provisioning and technology platforms are recited repeatedly in the Act's legislative history as the basis for its action and specific mechanisms put in place in 1994.[3]

> The purpose of H.R. 4922 is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies….
>
> To insure that law enforcement can continue to conduct authorized wiretaps in the future, the bill requires telecommunications carriers to ensure their systems have the capability….
>
> The legislation leaves it to each carrier to decide how to comply. A carrier need not insure that each individual component of its network or system complies with the requirements so long as each communication can be intercepted at some point that meets the legislated requirements.
>
> Section 2606 establishes a mechanism for implementation of the capability requirements that defers, in the first instance, to industry standards organizations.
>
> Carriers can adopt other solutions for complying with the capability requirements….
>
> The FCC retains control over the standards. Under section 2602(b), any carrier, any law enforcement agency or any other interested party can petition the FCC, which has the authority to reject the standards developed by industry and substitute its own.
>
> [T]he absence of standards will not preclude carriers, manufacturers or support service providers from deploying a technology or service, but they must still comply with the assistance capability requirements.
>
> Subsection (b) provides a forum at the Federal Communications Commission in the event a dispute arises over the technical requirements or standards. Anyone can petition the FCC to establish technical requirements or standards, if none exist, or challenge any such requirements or standards issued by industry associations or bodies under this section.
>
> If an industry technical requirement or standard is set aside or supplanted by the FCC, the FCC is required to consult with the Attorney General and establish a

[3] *See CALEA Legislative History* at 3495

> reasonable time and conditions for compliance with and the transition to any new standard. The FCC may also define the assistance obligations of the telecommunications carriers during this transition period.
>
> This section is also intended to add openness and accountability to the process of finding solutions to intercept problems.[4]

As we noted in April 2004 in conjunction with the joint federal agency petition for rule making in what became Docket 04-295 to develop and adopt the Commission's present rules for Communications Assistance for Law Enforcement Act and Broadband Access and Services, "[t]he only remedy here is Commission CALEA-based action so that the capabilities are in place."[5]

5. The Commission subsequently asserted its jurisdiction and authority provided by CALEA to IP broadband and interconnected telephony services. Its staff worked extensively over several years together with law enforcement agencies, industry, and congressional staff in domestic and international bodies to develop and agree on the necessary technical standards, and implemented them through the provisions in 47 CFR §§ 1.20000- 1.20008 adopted in 2006. The Commission's jurisdiction and actions were judicially sustained on appeal.[6] It seems well-settled that the Commission has the jurisdiction and authority pursuant to CALEA to act in the instant matter, including promulgation of its own standards. How it acts is the issue and challenge.

B. Adopted stable international LI/RD requirements and capability standards for 5G CALEA presently exist

6. The Commission at the outset of the Report & Order (R&O) bases its actions on the assertion that "[i]t is therefore vital that we protect these [5G] networks from national security threats."[7] It then proceeds to state that "the action we take today also implements section 105 of the Communications Assistance for Law Enforcement Act (CALEA) and cites numerous vulnerabilities and threats including "allowing equipment from untrusted suppliers to be part of a network."[8] It concludes that "[t]elecommunica-

[4] *Summary and Purpose, id.*
[5] Comments of Verisign, Inc, Dock. RM No. 10865, at 6, filed 12 April 2004.
[6] *See ACE v. FCC*, No. 05-1404 et al. (D.C. App. June 9, 2006)
[7] Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, Report and Order, Further Notice of Proposed Rulemaking, and Order, FCC 19-121 (2019) ("R&O") at para. 1
[8] *Id*. at para 35.

tions carriers, including all ETCs, therefore appear to have a duty to avoid such risks." The Commission does have the authority pursuant to CALEA to adopt its own standards – here in the form a prohibition to use of Universal Service Funds by a recipient telecommunication carrier for "equipment or services produced or provided by any company designated by the Commission as posing a national security threat to the integrity of communications networks or the communications supply chain."[9]

7. The conundrum being faced here is that for the past six years, vendors, providers and government authorities worldwide, including the FBI, have developed and adopted consensus-based 5G LI/RD requirements and implementation standards that address the known and anticipated threats and risks.[10] These are also very complex systems that are reflected in normative dependencies with multiple other industry-adopted 3GPP 5G LI/RD standards. Especially relevant is the recognition early-on among 5G security experts that 5G supply chains for LI/CALEA implementations represented a risk, and began work in 2014 in the NFV-SEC Industry Specification Group (ISG) to adopt a mitigating standard[11] that is mandated in the principal adopted 5G LI requirements standard.[12] These are authoritative 5G LI/RD standards intended for CALEA implementations developed by industry and law enforcement agencies and capable of being effectively implemented in products and services. However, it is not apparent that the Commission has considered them and found them insufficient as CALEA requires

C. The Commission's recently adopted CALEA standard for 5G is not implementable

8. By contrast, the Commission's sole CALEA standard published in the R&O – "not use…equipment or services [including software] produced or provided by any

[9] 47 CFR § 54.9(c), (d).
[10] See 3GPP, LI15, *Revised WID: Lawful Interception Rel-15*, SA SP-170839 (Dec 2017); LI16, *New WID: Lawful Interception Rel-16*, SA SP-181210 (Dec 2018); LI17, *New WID: Lawful Interception Rel-17*, SA SP-191337 (Dec 2019). The resulting specifications are TS 33.107, *Lawful interception architecture and functions*; TS 33.108, *Handover interface for Lawful Interception (LI)*; TS 33.126, *LI Service Requirements*; TS 33.127, *LI Architectures and Functions*; and TS 33.128, *LI delivery of required information to Law Enforcement Monitoring Facilities*.
[11] *See* ETSI GS NFV-SEC 012, *Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components*, 2017
[12] *See* 3GPP TS 33.126, *supra*.

company designated by the Commission" - is so vague that it is not capable of being understood, much less implemented.[13]

9. In 5G networks, there are multiple complex levels of equipment assemblies and services that are interconnected as part of virtualised global network architectures with innumerable virtual services that are orchestrated on demand. Signaling and software exchanges of all kinds necessary for management are constantly occurring. End user equipment and services are constantly moving and roaming. Most traffic is encrypted. Under the Commission's 5G CALEA rule, would an ECT U.S. service provider be precluded from interoperating with networks in China or many other places in the world where the *designated companies* had deployed equipment and services? How would the ECT provider detect where such equipment, software and services exist? How would the U.S. ECT service provider be able to detect and instantiate service to the millions of *designated company* devices, including chipsets, and services that exist or roam into their own service area? In 5G architectures, there are two basic layers – network and service. How does the Commission's standard apply to *designated company* equipment, software, and services in each of those layers and the interfaces between them? Mindful of this 5G architecture, what exactly is a 5G service provider under the Commission's new CALEA rule? How would an affected U.S. service provider comply with the rule? And lastly, how does the rule evolve with each of the new 5G specification releases? In short, the Commission's CALEA rule here is so disassociated from the reality of 5G networks and services that is it not implementable.

10. Furthermore, the degree of identification and isolation required to meet the Commission's 5G CALEA standard would necessitate an entirely different set of specifications for something that was different than the globally designed 5G found in the 3GPP specifications and it would have to be applied within small local U.S. enclaves that would essentially prevent any widespread communication or roaming. The implementation of such a 5G network would effectively place the U.S. in an electronic communications stone age.

[13] *Ref.* n. 9, *supra*.

C. The FCC should require universal implementation of existing trusted 5G LI/RD standards for CALEA rather than creating and adopting its own standards

11. For the past six years, experienced and knowledgeable lawful interception and security experts – drawn largely from North America and Europe and representing vendors, service providers, law enforcement, and national security organizations - have been working intensively on trusted 5G CALEA LI/RD specifications in open global standards activities.[14] The primary venue is SA3LI which is responsible for 5G LI /RD specifications, but also with outlying clusters of secondary and tertiary venues – especially peer 3GPP groups, TC LI, NFV SEC, MEC and TC CYBER.[15] The specifications are intended to meet CALEA and similar compliance provisions which exist in almost every country and region.

12. The specifications resulting from this several-year effort involving so many experts have been finely tailored to actually provide essential forensics and desired trust levels in the highly complex, dynamic, and extraterritorial 5G ecosystem. In other words, they are actually implementable. Location retained data is especially significant given the plethora of small cells and high-speed roaming being supported.[16] The virtualisation of everything and separation into network and service layers also necessitated new innovations like trusted virtualised points of interception supporting multiple law enforcement agencies that in turn necessitated special trusted LI-aware Management and Orchestration (MANO) features. The shift to non-IP protocols and multi-access edge computing required new means for capturing and identifying end-points and content. The massive bandwidth required new means of separating out and delivering LI content to law enforcement. The complexities and speeds also required reinvention of tasking using electronic warrants capable of being interfaced with judicial authorities.

13. Because supply chain trust from the outset was an important factor in a virtualisation environment, NFV SEC initially undertook that challenge six years ago and

[14] *See* n. 10, *supra*.
[15] The Technical Committees for Lawful Interception (TC LI) and Cyber Security (TC CYBER) together with the Industry Specification Groups for Network Functions Virtualisation Security (NFV SEC) and Multi-access Edge Computing (MEC) function as recognized public-private global standardization venues for normative specifications maintained by ETSI. ETSI also serves as the secretariat for 3GPP.
[16] Dynamic 5G location retained information is handled by a new subsystem known as Lawful Access Location Services (LALS).

produced effective solutions imported into 3GPP. The activity here occurred constantly – frequently with weekly virtual meetings – and includes extensive liaison outreach engagement with other bodies to instantiate needed 5G LI/RD component capabilities. The work is also tailored to the different versions of 5G as it evolves almost yearly pursuant to the specifications – Rel. 15, 16, 17, 18, etc. Rel. 15 is stable, and the focus in 2020 is on completing Rel. 16. All of this standards activity is also augmented by ISS World conferences four times a year rotating around the world - the principal tradeshow for implementing vendor 5G products.[17] FCC Commissioners and staff have not been involved in this activity since the 2004-2006 timeframe of the Docket 04-295 proceeding except for a short period three years ago by the Chief of the Public Safety and Homeland Security Bureau.

14. The Commission's assertion of its CALEA jurisdiction and authority for 5G is timely and appropriate. However, instead of going forward with any of its own standards, the Commission should first assess and implement the CALEA capabilities specified in the existing 5G LI/RD standards produced through this six-year government-private sector effort in venues recognized by the Commission in 2006 and relied upon globally by Commission counterparts. If any additional U.S. national options are needed, the Commission should work with the FBI and industry and engage in the 5G LI/RD these public-private standards activities to perfect those options and enable vendors and service providers to implement them. It is likely the FCC engagement would be welcomed again by its peers as it engaged in this work, and it would facilitate availability of the considerable knowledge base found in the venues. Because 5G architectures and networks are so fundamentally different – using non-IP protocols with different end-point identifiers and resolvers, diverse extraterritorial architectures orchestrated on demand, multi-access edge computing – the Commission is unlikely to possess the expertise to understand the evolving CALEA requirements.

15. What is especially important at this juncture, is for the Commission through its CALEA rulemaking authority, to require that all the 5G service providers and vendors implement the industry adopted global 5G LI/RD specifications and the evolving versions in the various 5G releases. In a highly complex and dynamic 5G ecosystem, the CALEA requirements go far beyond just supply chain concerns. Such FCC action would

[17] *See* Telestrategies, https://www.telestrategies.com/.

likely to be especially welcomed by U.S. law enforcement authorities and their counterparts in other venues who are all struggling to maintain needed investigative capabilities in a 5G world. It seems unfathomable that with the disbursement of billions of dollars in USF funds to ECTs for new 5G equipment, support for adopted 5G LI/RD specifications would not be required.

D. The Commission should enable USF monies for independent domestic Trust Third Party CALEA services

16. As the Commission recognized fourteen years ago in the Docket 04-295 CALEA proceeding, implementing the requisite capabilities is a difficult challenge for rural and underserved providers who are ECTs. Yaana's NetDiscovery® Services product was advanced as a highly viable option for this group – resulting in Trusted Third Party (TTP) implementations being included not only in the Commission's CALEA rules, but also in the international LI/RD industry standards. For the complex, new, constantly evolving 5G services ecosystem, meeting the adopted 5G LI/RD specifications may be a challenge - especially for ECTs. Fortunately, Trusted Third Party providers of those capabilities like Yaana exist in their own competitive marketplace, and as an ideal option for any provider which cannot meet the requirements or outsource the responsibilities.

17. TTPs have a significant additional value proposition in the context of the instant proceeding because they can provide an array of additional compliance and security services – especially discovering suspicious surreptitious exterritorial or domestic configuration changes or service orchestrations. Such threats can occur with any vendor equipment, software and services – and many if not most smaller service providers are unlikely to have the capabilities to detect and thwart them.

18. In light of TTP options available to meet not only CALEA 5G LI/RD requirements, but also address the national security concerns threats raised above, the Commission should make USF monies available to TTPs as "CALEA services ECTs" – either directly or as an allowable expense of any ECT.