PUBLIC SUBMISSION

As of: January 14, 2020
Received: January 05, 2020
Status: Pending_Post
Tracking No. 1k4-9e9j-499n
Comments Due: January 10, 2020
Submission Type: Web

Docket: PTO-C-2019-0038
Request for Comments on Intellectual Property Protection for Artificial Intelligence Innovation

Comment On: PTO-C-2019-0038-0002
Intellectual Property Protection for Artificial Intelligence Innovation

Document: PTO-C-2019-0038-DRAFT-0010
Comment on FR Doc # 2019-26104

Submitter Information

Name: Syamantak Saha
Address:
HA 8 Salt Lake City
Kolkata, West Bengal, India, 700097
Email: syamsaha@ieee.org
Phone: +919830815425

General Comment

As technology advancements, contemporarily, are largely developed with digital technologies and for a digital economy, an important critical infrastructure for this are the telecommunication technologies of a State. As the developing Internet-of-Things and IPv6 are foundational for the next generation digital economy, technologies including Artificial Intelligence applications that form the basis for such telecommunication developments have to be protected by the United States and for its Allies, such as the safety, security and reliability of important telecommunication, that dirrectly affects national security operations, are not easily procured, transmitted or analysed for vulnerability exploitation by adversaries.

Whilst several Artificial Intelligence methods such as Neural Networks etc., are listed on the sensitive technology list for export control, what is critically missing are related IoT, IPv6 and communications engineering technologies such as TCP/IP advancements that will be foundational for telecommunication developments in the near future.

A important addendum to the list would be a functionally defined list as well, that includes direct application to telecommunication engineering. So, any Artificial Intelligence technology and its related research and advancements, if applicable and critical for telecommunication protocol engineering, should be added to the sensitive technology and export control list.

Today, the United States and its allies are largely exposed to the previous uncontrolled availabilities of the functionally telecommunication based technologies, such as TCP/IP, VoIP and similar technologies that has resulted in potential state sponsored cyberterrorism and various other forms of attack, that compromise vital information and e-space of the US and Allies. Taking a functionally based approach to listing sensitive and export controlled technologies would certainly assist in preventing future digital economy safety and security

features.