Wilson Llivichuzhca
11670 Carroll Mill Rd.
Ellicott City, MD 21042
410-412-9333
llivichuzhca@gmail.com

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Subject: Proposed amendment to IEEE Std 802.1AE™-2018

To whom it may concern,

I write to propose an amendment to the IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security (IEEE Std 802.1AE™-2018). The last paragraph on page 8 of the aforementioned standard states: "IEEE Std 802.1AE is not intended for use with IEEE Std 802.11™." This sentence precludes the implementation of MACsec encryption in 802.11 wireless networks and, I believe, should be reworded or removed from the publication.

Some government and military use cases require two approved layers of encryption for 802.11™ wireless communications. MACsec, WPA2 and WPA3 are some approved encryption methods. It has been proven that implementing software-based MACsec on top of WPA2 or WPA3 provides two layers of approved encryption. However, the mentioned sentence is precluding the use of this viable combination. The sentence in question is not a strong reason for not implementing a solution using MACsec over WPA2/3 and (as noted by the first sentence on the page) it is not part of the standard. However, government and military organizations take every part of the publication as the standard itself, thus they reject the use of MACsec on wireless networks based on the 802.11™ standard.

I recommend the removal of the mentioned sentence from the publication or reword it in such a way that does not preclude the use of MACsec in combination with WPA2/3.

Thank you for your consideration.

Sincerely,

Wilson Llivichuzhca