IEEE 802.3 Ethernet Working Group
DRAFT Liaison Communication

Source:	IEEE 802.3 Working Group[1]	
To:	Jungyup Oh	ISO/IEC JTC 1/SC 6 Secretariat [redacted]
CC:	Alpesh Shah	Secretary, IEEE-SA Standards Board Secretary, IEEE-SA Board of Governors [redacted]
	James Gilb	Chair, IEEE 802 LMSC [redacted]
	Adam Healey	Vice-chair, IEEE 802.3 Ethernet Working Group [redacted]
	Jon Lewis	Secretary, IEEE 802.3 Ethernet Working Group [redacted]
	Peter Yee	Chair, IEEE 802 JTC1 Standing Committee [redacted]
From:	David Law	Chair, IEEE 802.3 Ethernet Working Group [redacted]
Subject:	Liaison reply to China National Body comments during the ISO/IEC JTC 1/SC 6 Committee Internal Ballot 'Submission of IEEE 802.3-2022'	
Approval:	Agreed to at IEEE 802.3 interim teleconference meeting, 16 May 2024	

Dear ISO/IEC JTC 1 SC 6 Secretariat,

The IEEE 802.3 Ethernet Working Group thanks the China National Body for their review and comments during the ISO/IEC JTC 1/SC 6 Committee Internal Ballot regarding the submission of IEEE Std 802.3-2022 for adoption under the ISO/IEEE Partner Standards Development Organization (PSDO) agreement.

Please find below the comments and proposed changes as received, followed by the responses from the IEEE 802.3 Ethernet Working Group.

Sincerely,
David Law
Chair, IEEE 802.3 Ethernet Working Group

[1] This document solely represents the views of the IEEE 802.3 Working Group and does not necessarily represent a position of the IEEE, the IEEE Standards Association, or IEEE 802.

Comment CN1	IEEE 802.3-2022 is a new edition of IEEE 802.3-2018 after merged IEEE 802.3cb-2018、802.3bt-2018、802.3cd-2018、802.3cn-2019、802.3cg-2019、802.3cq-2020、802.3cm-2020、802.3ch-2020、802.3ca-2020、802.3cr-2021、802.3cu-2021、802.3cv-2021、802.3ct-2021 and 802.3cp-2021. For IEEE 802.3-2018 and its amendments, China has made several comments on their security technologies, unfortunately, we have not seen any efforts in the new edition to improve the security of the proposal, and IEEE 802.3-2022 still lacks specification of Ethernet security technology, which neither contains security mechanisms and security technology features nor normative references to other security technologies. In response, the IEEE 802.3 Working Group has been claiming that the standard is "security agnostic" and that implementers can use any security mechanism. In fact, security mechanisms are an integral part of networking standards, and Ethernet security is an important part of cyberspace security. The lack of security mechanisms exposes Ethernet to security threats such as device forgery, communication theft, and tampering. Due to the lack of necessary specifications and guidance in the proposal, when an implementer chooses any security mechanism, in addition to the interoperability and compatibility issues that will be brought about by the products and network interconnections, if the security mechanism it chooses is inherently insecure, it will lead to security risks and vulnerabilities in the network systems that will be implemented in accordance with these standards. IEEE 802.3 allows for any security mechanism to be applied to Ethernet, which will weaken its security and jeopardize other networks, with disastrous consequences.
Proposed change	It is strongly suggested that IEEE 802.3 and its amendments specifying security mechanisms.
Response	The scope of IEEE 802.3 does not include the setting of provisions for, or providing guidance about, security. IEEE 802.3 is security agnostic and allows the user to run any security protocol over an Ethernet network that satisfies that user’s security requirements. This approach enables the users of Ethernet networks to select the correct security mechanism, from those available at the time, and at the correct level (e.g., link, application) to satisfy the user’s security requirements.

DRAFT

Comment CN2	We understand that at least six IEEE negative Letters of Assurance (LoAs, equivalent to an ISO type 3 declaration) have been made regarding the IEEE 802.3 specification. It is deviant with ISO/IEC patent policy. JTC 1 shall not permit the proposal to enter “fast tracking” process where there is no assurance of licensing/access to IEEE specifications, as instructed by ISO/TPM and SC6 CM.
Proposed change	-
Response	Contribution 6N18159 ‘Revised ISO update on patent declarations and IEEE adoptions – December 2023’ from ISO TPM includes: *It is further noted that IEEE and ISO have separate patent policies, and in particular during the current adoption process where IEEE submits a published IEEE standard to ISO/IEC JTC1/SC6 (or another JTC1 Subcommittee) for publication as an ISO/IEC/IEEE International Standard, ISO and IEC through the common patent policy are required to review the status of patent declarations.* Contribution 6N18159 also includes ‘*However, the current patent policy in ISO/IEC/ITU remains unaffected, requiring relevant committees to review the status of patents on IEEE adoption proposals to determine if patent declarations under the ISO/IEC/ITU patent policy need to be filed. If a negative LoA patentholder is unable or unwilling to grant license to use the patented content in accordance with the ISO/IEC/ITU patent policy (either by email refusal, patent declaration form Option 3 filed, or no response), ISO and IEC are unable to publish the adopted ISO/IEC/IEEE standard.* A CIB ballot of the submission of IEEE Std 802.3-2022 was announced on 27 April 2023 but was cancelled a few hours later accompanied by the statement ‘*Unfortunately, I inform you that the IEEE 802.3-2022 CIB, which was scheduled for balloting on April 27th, 2023, has been canceled. This is due to the discovery of negative Letters of Assurance (LoA) associated with this standard, and as a result, the ballot cannot proceed.*’ from the ISO/IEC JTC 1/SC 6 committee manager. This new CIB ballot of the submission of IEEE Std 802.3-2022 was announced on 17 February 2024 including the note ‘*ISO CS completed the patent declaration review and patent declaration database has been updated at ISO - ISO Standards and Patents (https://www.iso.org/iso-standards-and-patents.html).*’. Based on this sequence of events, and contribution 6N18159, it would seem that the necessary patent declarations under the ISO/IEC/ITU policy are now available in the ISO patent declaration database at the referenced URL.

DRAFT