



ISO/IEC JTC 1/SC 27/WG 3 "Security evaluation, testing and specification"

Convenorship: UNE

Convenor: Bañón Miguel Mr



PWI Proposal - Emerging Technologies

Document type	Related content	Document date	Expected action
Project / Other	Meeting: VIRTUAL 14 Sep 2026 Project: ISO/IEC PWI 25240	2026-09-17	INFO

PWI on Evaluation of Emerging and Recent Technologies Including AI

Background:

- Frontier AI has changed the technological landscape. Advanced AI systems can exhibit emergent and agentic behaviors beyond explicitly trained functions. The 2026 OpenAI-Hugging Face incident demonstrated this by chaining vulnerabilities, bypassing isolation controls, communicating through unauthorized channels and accessing third-party systems. These types of autonomous behaviors challenge traditional Common Criteria threat models and operational assumptions.
- Advances in Quantum Computing have already accelerated the U.S. federal migration timelines. The concern is not just the future ability of quantum computers to break current cryptography, but also the "harvest now, decrypt later" risk of adversaries collecting sensitive information for future decryption. In July 2026, Anthropic reported that an AI model discovered a vulnerability in the HAWK candidate which led to its withdrawal from NIST consideration. Evaluations may need to examine quantum-related risks including cryptographic agility, protocols, keys and implementation.
- Supply chain risk is amplified by AI. Widespread use of open source software, including deprecated and unmaintained components has created opportunities for exploitation. In addition, AI's ability to discover and chain vulnerabilities, as well as rapidly create exploits has increased the need to modernize the vulnerability disclosure system. Bills of Materials (BOMs) such as Software (SBOM), Hardware (HBOM), Cryptography (CBOM) and AI/ML (AI/ML-BOM) provide greater visibility into risks. However, BOM methodologies are not yet mature – different SBOM generation tools identify different components and the data quality of generated SBOMs is usually insufficient. SBOMs and vulnerability handling are requirements in the EU Cyber Resilience Act with further specifications in CEN/CENELEC's EN 4000-1-3.

Proposed Scope:

This PWI serves as an incubator for other PWIs on how to enhance (ISO/IEC 15408 and 18045, ISO/IEC 19790/24759) for security evaluation of emerging and recent technologies. This may include but is not limited to Security Functional Requirements, Security Assurance Requirements, Evaluation Methodology, Attack Potential, the Target of Evaluation or any other concept in the aforementioned documents or not yet part of the current standards.