

LIAISON STATEMENT

FROM: ISO/IEC JTC 1/SC 27/WG 3
TO: The CCUF

Appreciation

ISO/IEC JTC 1/SC 27/WG 3 thanks the CCUF for their liaison statement circulated as ISO/IEC JTC 1/SC 27/WG 3 N2368 dated 3rd October, 2022. The WG 3 thanks to the CCUF for the updates of organization status, scope of interest, and the dates of its forthcoming meetings. These are noted and WG 3 requests that the CCUF continue to include information about their future meetings in their future liaison statements.

Publication progress - ISO/IEC 15408, ISO/IEC 18045, and TR22216

WG 3 experts were informed by the WG 3 convenor and the CCDB liaison officer that discussions regarding the IPR/copyright issues for the revision has been satisfactorily resolved and that progress is also being made in discussions to place the agreement on a permanent footing to cover future revisions. The WG 3 experts were pleased to hear this and grateful for those, in all organizations, working on the subject.

Notice of publication - ISO/IEC 15408, ISO/IEC 18045, TR22216 and others

The followings have been published and is now available through the National Standard Bodies, ISO and IEC.

- ISO/IEC 15408-1:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model"
- ISO/IEC 15408-2:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components"
- ISO/IEC 15408-3:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components"
- ISO/IEC 15408-4:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities"
- ISO/IEC 15408-5:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements"
- ISO/IEC 18045:2022 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation"
- ISO/IEC TR 22216:2022 "Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022"
- ISO/IEC TR 5895:2022 "Cybersecurity — Multi-party coordinated vulnerability disclosure and handling"

Preliminary work item: Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045

The aim of project "PWI 7677 Roadmap for the maintenance of ISO/IEC 15408 and ISO/IEC 18045" was to produce a roadmap for the future development of the standards. The WG 3 has updated the roadmap and discussions were held during the SC 27/WG 3 meeting week. The working group experts finally agreed that the roadmap provided by PWI 7677 will serve as a starting point for future investigation and implementation. In addition, a new preliminary work item titled "*Investigation of the feasibility and implementation of changes to ISO/IEC 15408 and ISO/IEC 18045*" has been proposed. The scope of this PWI covers any work needed to gain consensus within WG 3 for both the contents and the implementation of the changes. It will provide the overall coordination and project management needed to ensure a coherent set of changes and smooth, successful set of revision to the ISO/IEC 15408 and ISO/IEC 18045. WG 3 would

welcome inputs from the CCUF at any point and, in particular, any suggestions arising from their use of the updated standards.

Current status on specific product types: cryptographic modules

The 4th edition of **ISO/IEC 19790** (“Security requirements for cryptographic modules”) is currently under revision. It specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication system. ISO 19790 defines four security levels for cryptographic module to provide for a wide spectrum of data sensitivity and diversity of application environments. ISO/IEC 19790 specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level. The 4th edition of **ISO/IEC 24759** (“Test requirements for cryptographic modules”) is currently under revision, in parallel to ISO/IEC 19790. It specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories. It also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules’ conformity to the requirements specified in ISO/IEC 19790.

Due to the reception of a large number of comments against 19790 4th WD and 24759 4th WD, the expert discussion and disposition of comments had been started ahead of the WG 3 plenary. The followings topics have been discussed during this meeting; Device Attestation, Multi-factors Authentication, Manufacture CSPs, Modifiable OE, SSPs establishment and entry/exit, Zeroization requirements, Physical security requirements, Finite State Model requirements etc.

General

We look forward to continuing the rewarding relationship with the CCUF and encourage the CCUF to provide any CCUF work items that the working group may consider for review. Please note that the latest status of all WG 3 projects, the relevant document numbers, and the schedule for updates and comments are all to be found in the WG 3 recommendations document that is attached to this liaison statement. Documents of interest to the CCUF are made available through the liaison channel with SC 27/WG 3.

Future meetings

WG 3 includes information regarding its future meetings and would like to inform the CCUF of the following events planned for 2023.

- 17-21 April 2023, The 79th ISO/IEC JTC 1/SC 27/WG 3 meeting, Redmond, United States

Attachments

ISO/IEC JTC 1/SC 27/WG 3 Recommendations, 78th Meeting