LIAISON STATEMENT

FROM: ISO/IEC JTC 1/SC 27/WG 3

TO: The CCUF

# **Overview and 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 N2639 dated 9th April, 2024. The WG 3 thanks to the CCUF for the updates of organization status, scope of interesting, 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.

# **Progress of ISO/IEC 15408 and 18045 revisions**

The editors group and other experts met during the ISO/IEC JTC 1/SC 27/WG 3 meeting week and produced draft DoCs (Disposition of Comments) for comments that had been made on the 1st working drafts. These will be used for the editing process for DIS which is planned to complete by 2024-06-01.

The editors wanted to put on record their particular thanks to the CCUF/CCDB participants, and to the CCMB joint chairs, Ms. Eunkyoung Yi and Dr. Susanne Pingel, who performed a great deal of comment preparation work in a very timely manner.

# **Publication of ISO/IEC TS 9569:2023**

SC27/WG3 is happy to inform the CCUF that the technical specification *ISO/IEC TS 95569: 2023 Information security, cybersecurity and privacy protection ─ Evaluation criteria for IT security ─*

*Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045* was published November, last year. We hope this specification would support the CC community in developing effective approach to the patch management issue which is relevant to the ICT product evaluations.

# **Items highlighted as likely to be of particular interest to the CCUF**

Please note that the latest status of all WG 3 projects, relevant document numbers, and the schedule for updates and comments are all to be found in the resolutions document that is attached to this liaison statement. Documents of interest to the CCUF can be made available through the liaison channel with SC 27. We would like to draw your attention to the following projects:

# **Proposal for revision of ISO/IEC 19989-1:2020 Information security Criteria and methodology for security evaluation of biometric systems Part 1: Framework**

It was recommended that the Project Editors/Co-Editors prepare a 1st WD for this part of the standard.

# **ISO/IEC 19896 (3 parts) IT security techniques — Competence requirements for information security testers and evaluators**

The current status of this multipart project is the following:

* Part 1: Introduction and concepts,
* Part 2: Knowledge and skills requirements for ISO/IEC 19790 testers and validators, both have reached the DIS (Draft International Standard) stage.
* Part 3: Knowledge and skills requirements for ISO/IEC 15408 evaluators and certifiers – has reached the CD (Committee Draft) stage.

# **Preliminary Work Item proposals**

SC27/WG3 has decided to start several preliminary work items i.e.:

* Evaluation of AI-based technology, with proposed scope:
* To examine and propose AI-specific Threats, Organization Security Policies, Assumptions, and Security Objectives for various types of AI attack types and techniques. The scope will be further defined/refined if the project is started.
* To develop extended AI-specific Security Functional Requirements (AI-SFRs) and AI-specific Security Assurance Requirements (AI-SARs) to counter the identified AI attack types and techniques.
* To develop evaluation methodology to verify the efficiency and sufficiency of the AI-SFRs and AI- SARs.
* Support for customized or multipurpose evaluation:
* A review of cybersecurity requirements and related evaluation methodologies with a view to provide recommendations on the following actions.
* A review of cybersecurity evaluation and certification process.
* An analysis of reusability.
* The provision of a report and recommendations for future standardization work.

as experts in evaluation and certification the CCUF may wish to provide input (or encourage evaluation labs to provide input) for the call for contributions involved in these.

# **EU developments in the area of cybersecurity evaluation methodologies**

The working group was briefed on two EU developments that have relevance to international standardization of security assurance: EN 17640 “Fixed-time cybersecurity evaluation methodology for ICT products” and EN 17927 “Security Evaluation Standard for IoT Platforms”.

# **Notice of publication**

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

* ISO/IEC TR 5891:2024 Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment
* ISO/IEC TS 9569:2023 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045
* ISO/IEC 17825:2024 Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules
* ISO/IEC TS 24462:2024 Information security, cybersecurity and privacy protection — Ontology building blocks for security and risk assessment

# **Future meetings**

WG 3 includes information regarding its future meetings and would like to inform the CCUF of the following events planned for 2024.

* The 84th ISO/IEC JTC 1/SC 27/WG 3 meeting
  + Date: 30th September - 4th October 2024

# **Attachments**

* ISO/IEC JTC 1/SC 27/WG 3 Recommendations, 83rd Meeting

Regards,  
  
Liaison Officer from SC 27/WG 3 to the CCUF  
Kwangwoo Lee