

## WG 23 Liaison Report to SC 22/WG 9 ISO/IEC/JTC 1/SC 22 WG23 N0661

---

### WG23 Liaison Report:

Since the last WG9 meeting in Vermont, WG23 has met in five 2-hour teleconferences and two face-to-face-meetings. The main subject of the work of WG23 over the past six months has been the Vulnerabilities document, now split into 8 parts. SC22 apparently has agreed to the split, since individual parts show up on the official ISO lists of ongoing work.

The TeleCons (Oct. 21<sup>st</sup>, Nov. 23<sup>rd</sup>, Feb. 8<sup>th</sup>, March 7<sup>th</sup>, May 16<sup>th</sup>) mainly served to review and integrate changes made to the documents in response to assignments made at previous meetings. Also, upcoming face-to-face meetings were prepared.

At the face-to-face meeting in Orlando, Florida, Jan. 11<sup>th</sup> + 12<sup>th</sup>, TR-24772 was reviewed in light of comments and additions received and not yet handled. Action items for the development of wording were assigned. Updates to the cross-references to the evolving CWE, to JSF, Misra and C CERT rules or vulnerabilities were initiated. Remaining decisions about the structure of the language-specific Parts of the TR were made, e.g., about the contents of the split-up Bibliography (where each Part shall contain its own references and only those). For the C-Annex, a new section with the “top N Guidelines” (N = ~10 or 12, “Dirty Dozen”) was drafted. A similar attempt for Ada was initiated. The C++ Code Guidelines and their interrelationship with TR-24772 were examined: some are useful to cover vulnerabilities, but there are many C++ guidelines that have different objectives such as code efficiency or software engineering concerns. While worthwhile, many of these guidelines are outside the scope of WG23 work. TS 17961, the C Secure Coding Rules, which was recently amended with a Technical Corrigendum, was discussed in the same context.

At the face-to-face meeting at the BSI offices in London, April 15<sup>th</sup> and 16<sup>th</sup>, the cooperation with WG14 was explored in more detail. A partially joint meeting of WG14 and WG23 before the main WG23 meeting discussed various apprehensions that WG14 members wanted to voice. At the WG23 meeting, we listed the many documents for C coding guidelines in existence today and discussed to what extent we should cite and use them. The role of Section 7 was examined in connection with the newly added time-related vulnerabilities. The latter were eventually moved into Section 7 as environment-related vulnerabilities hardly caused or prevented by programming language elements. Section 7 vulnerabilities should be reordered by general categories to provide a better flow to the reader. (As Section 7 plays no role in the language-dependent parts, WG9 is not affected by this work.)

In the next few months, the monthly TeleCons will continue. Face-to-face meetings are planned for Vienna in September and Florida in January of 2017.

WG23 thanks WG9 for its efforts in updating the old Annex to become Part-3 of TR-24772 and expresses its hopes to receive the document from WG9 for the WG23 meeting starting on June 14<sup>th</sup>.