International Organization for Standardization
Organisation internationale de normalisation
Международная организация по стандартизации

FORM 4:
NEW WORK ITEM PROPOSAL (NP)

Circulation date Click here to enter a date. **Closing date for voting** Click here to enter a date.	**Reference number:** Enter Number (to be given by ISO Central Secretariat) **ISO/IEC**/JTC 1/**SC** 22 ☐ Proposal for a new PC **SC 22/WG 23/N 1095**
Proposer ☐ ISO member body: Click here to enter text. ☒ Committee, liaison or other[1]: Click here to enter text.	
Secretariat Click here to enter text.	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee.

[1]The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General. See ISO/IEC Directives Part 1, Clause 2.3.2.

The proposer(s) of the new work item proposal shall:
- make every effort to provide a first working draft for discussion, or at least an outline of a working draft;
- nominate a project leader;
- discuss the proposal with the committee leadership prior to submitting the appropriate form, to decide on an appropriate development track (based on market needs) and draft a project plan including key milestones and the proposed date of the first meeting.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

IMPORTANT NOTE
Proposals without adequate justification risk rejection or referral to originator.

Guidelines for proposing and justifying a new work item are contained in Annex C of the ISO/IEC Directives, Part 1.

☒ The proposer has considered the guidance given in the Annex C during the preparation of the NP.

Resource availability:
☒ There are resources available to allow the development of the project to start immediately after project approval* (i.e. project leader, related WG or committee work programme).

* if not, it is recommended that the project is first registered as a preliminary work item (a Form 4 is not required for this) and when the development can start, Form 4 should be completed to initiate the NP ballot.

Proposal (to be completed by the proposer, following discussion with the committee leadership)

Title of the proposed deliverable

English title

Programming languages – Guidance to avoiding vulnerabilities in programming languages – Part 1: Language independent guidance

French title (if available)

Langages de programmation — Conduite pour éviter les vulnérabilités dans les langages de programmation — Partie 1: Conduite indépendante du langage

(In the case of an amendment, revision or a new part of an existing document, include the reference number and current title)

Scope of the proposed deliverable

This document catalogues common software programming language vulnerabilities and their mitigations in the development of systems where assured behaviour is required for security, safety, mission-critical and business-critical software. In general, this guidance is applicable to the software developed, reviewed, or maintained for any application.
This document is Part 1 of a series. Vulnerabilities and their mitigations are described in this document in a generic manner that is applicable to a broad range of programming languages.
This document is supplemented by other Parts in this series that describe how vulnerabilities catalogued in this document arise and how they can be mitigated in specific programming languages, such as C, C++, Ada, Java, Python, SPARK, and Fortran.

Purpose and justification of the proposal

The material to be standardised has existed as an International Technical Report 24772 since 2010 and has been revised and enhanced in 2012 and in 2019-20 to include more vulnerabilities and additional programming languages.

The existence of the earlier documents and the support of the international community for this work since 2008 clearly shows that the community values the work.

Ever since programming languages were created, the technical community has been concerned about programming practices and coding errors. Such errors can result in the program being compromised in ways that can lead to program crashes, freeze-ups, or the program being attacked and potentially taken over. Each of these events can lead to any level of damage to the system that contains the application up to and including the loss of the system.

This Standard documents how such programming mistakes can occur, and how they are influenced by choices made by the programmer, the system architect or by the programming language designer. It provides identification of the consequences of such errors and guidance on their mitigations.

By using the guidance provided in this document, systems can be produced that are safer, more secure and more robust. Many of the attacks on digital systems as well as common system design and programming mistakes can be avoided.

A change in ISO/IEC rules has excluded Technical Reports from free availability. Converting the Technical Report to an International Standard will permit this edition to qualify to be freely available as were the first two editions of the TR.

Please select any UN Sustainable Development Goals (SDGs) that this document will support. For more information on SDGs, please visit our website at www.iso.org/SDGs."

☐ **GOAL 1:** No Poverty
☐ **GOAL 2:** Zero Hunger
☒ **GOAL 3:** Good Health and Well-being
☒ **GOAL 4:** Quality Education
☐ **GOAL 5:** Gender Equality
☐ **GOAL 6:** Clean Water and Sanitation
☐ **GOAL 7:** Affordable and Clean Energy
☐ **GOAL 8:** Decent Work and Economic Growth
☒ **GOAL 9:** Industry, Innovation and Infrastructure
☐ **GOAL 10:** Reduced Inequality
☐ **GOAL 11:** Sustainable Cities and Communities
☒ **GOAL 12:** Responsible Consumption and Production
☐ **GOAL 13:** Climate Action
☐ **GOAL 14:** Life Below Water
☐ **GOAL 15:** Life on Land
☐ **GOAL 16:** Peace and Justice Strong Institutions
N/A **GOAL 17:** Partnerships to achieve the Goal

Preparatory work
(An outline should be included with the proposal)

☒ A draft is attached
☐ An outline is attached
☐ An existing document will serve as the initial basis

The proposer or the proposer's organization is prepared to undertake the preparatory work required: ☒ Yes ☐ No

If a draft is attached to this proposal

Please select from one of the following options (note that if no option is selected, the default will be the first option):
☐ Draft document can be registered at Working Draft stage (WD – stage 20.00)
☐ Draft document can be registered at Committee Draft stage (CD – stage 30.00)
☒ Draft document can be registered at Draft International Standard stage (DIS – stage 40.00)

☐ If the attached document is copyrighted or includes copyrighted content, the proposer confirms that copyright permission has been granted for ISO to use this content in compliance with clause 2.13 of the ISO/IEC Directives, Part 1 (see also the Declaration on copyright).

Is this a Management Systems Standard (MSS)?

☐ Yes ☒ No

NOTE: if Yes, the NP along with the Justification study (see Annex SL of the Consolidated ISO Supplement) must be sent to the MSS Task Force secretariat (tmb@iso.org) for approval before the NP ballot can be launched.

Indication of the preferred type or types of deliverable to be developed

☒ International Standard
☐ Technical Specification
☐ Publicly Available Specification

Proposed Standard Development Track (SDT)

To be discussed between proposer and Secretary considering, for example, when does the market (the users) need the document to be available, the maturity of the subject etc.

☒ 18 months* ☐ 24 months ☐ 36 months ☐ 48 months

* Projects using SDT 18 are eligible for the 'Direct publication process' offered by ISO /CS which reduces publication processing time by approximately 1 month.

Draft project plan (as discussed with committee leadership)

Proposed date for first meeting: Two months after NWIP approval

Proposed dates for key milestones:
1st Working Draft (if any) circulated to experts: N/A
Committee Draft ballot (if any): N/A
DIS submission*: Simultaneous with NWIP
Publication*: 2022-10-01

* Target Dates on DIS submission and Publication should preferably be set a few weeks ahead of the limit dates (automatically given by the selected SDT).

For guidance and support on project management; descriptions of the key milestones; and to help you define your project plan and select the appropriate development track, see: go.iso.org/projectmanagement

NOTE: The draft project plan is later used to create a detailed project plan, when the project is approved.

Known patented items (see ISO/IEC Directives, Part 1, clause 2.14 for important guidance)

☐ Yes ☒ No

If "Yes", provide full information as annex

Co-ordination of work
To the best of your knowledge, has this or a similar proposal been submitted to another standards development organization?

☐ Yes ☒ No

If “Yes”, please specify which one(s):

Click here to enter text.

A statement from the proposer as to how the proposed work may relate to or impact on existing work, especially existing ISO and IEC deliverables. The proposer should explain how the work differs from apparently similar work, or explain how duplication and conflict will be minimized

This work is a growth of the work already done by JTC 1/SC 22/WG 23 and will result in the work currently published as a Technical Report being extended and published as an International Standard.

A listing of relevant existing documents at the international, regional and national levels

ISO/IEC TR 24772-1:2019 Programming languages – Guidance to avoiding programming language vulnerabilities – Part 1: Language independent guidance
ISO/IEC TR 24772-2:2020 Programming languages – Guidance to avoiding programming language vulnerabilities – Part 2: Ada
ISO/IEC TR 24772-3:2020 Programming languages – Guidance to avoiding programming language vulnerabilities – Part 3: C

Please fill out the relevant parts of the table below to identify relevant affected stakeholder categories and how they will each benefit from or be impacted by the proposed deliverable(s)		
	Benefits/impacts	**Examples of organizations/companies to be contacted**
Industry and commerce – large industry	Since all industries program computers, using these standards will improve their resistance to failures due to programming mistakes and attack	Organizations interested in the safety and security of their products that contain any IT.
Industry and commerce – SMEs	Since all industries program computers, using these standards will improve their resistance to failures due to programming mistakes and attack	Organizations interested in the safety and security of their products that contain any IT.
Government	Since governments purchase programs written for their computers, having suppliers use these standards will improve their resistance to failures due to programming mistakes and attack	Any government organization with vested interest in the safety and security of the general population. Government agencies that acquire and use IT-based systems.
Consumers	Click here to enter text.	Click here to enter text.
Labour	Click here to enter text.	Click here to enter text.
Academic and research bodies	Safety and security of IT-based systems are an important and active research area.	Research organizations that are working on improving the safety and security of IT-based systems. Educators in teaching safe programming practices.
Standards application businesses	Click here to enter text.	Click here to enter text.
Non-governmental organizations	Click here to enter text.	Click here to enter text.
Other (please specify)	Click here to enter text.	Click here to enter text.

Liaisons A listing of relevant external international organizations or internal parties (other ISO and/or IEC committees) to be engaged as liaisons in the development of the deliverable(s). WG 23 currently maintains liaisons with all other SC 22 programming language groups, external language committees, security committees such as JTC 1/SC 27, and industry safety groups such as MISRA	**Joint/parallel work** **Possible joint/parallel work with** ☐ IEC (please specify committee ID) Click here to enter text. ☐ CEN (please specify committee ID) Click here to enter text. ☐ Other (please specify) Click here to enter text.
A listing of relevant countries which are not already P-members of the committee Click here to enter text. **NOTE:** The committee manager shall distribute this NP to the ISO members of the countries listed above to ask if they wish to participate in this work	
Proposed Project Leader (name and e-mail address) Stephen Michell, Canada stephen.michell@maurya.on.ca	**Name of the Proposer** (include contact information) Stephen Michell, Canada stephen.michell@maurya.on.ca
This proposal will be developed by ☒ An existing Working Group (please specify which one: JTC 1/SC 22/WG 23) ☐ A new Working Group (title: Click here to enter text.) (Note: establishment of a new WG must be approved by committee resolution) ☐ The TC/SC directly ☐ To be determined	
Supplementary information relating to the proposal ☐ This proposal relates to a new ISO document; ☐ This proposal relates to the adoption as an active project of an item currently registered as a Preliminary Work Item; ☐ This proposal relates to the re-establishment of a cancelled project as an active project. ☒ Other: This proposal is for a conversion and minor revision of an existing ISO/IEC Technical Report for publication as an International Standard.	

Maintenance agencies (MA) and registration authorities (RA)

☐ This proposal requires the service of a **maintenance agency**.
If yes, please identify the potential candidate:
Click here to enter text.

☐ This proposal requires the service of a **registration authority**.
If yes, please identify the potential candidate:
Click here to enter text.

NOTE: Selection and appointment of the MA or RA is subject to the procedure outlined in the ISO/IEC Directives, Annex G and Annex H, and the RA policy in the ISO Supplement, Annex SN.

☒ Annex(es) are included with this proposal (give details)

Draft document for concurrent DIS ballot is attached.

Additional information/questions

Click here to enter text.