



ANSI/CAN/UL 2900-1:2023

JOINT CANADA-UNITED STATES
NATIONAL STANDARD

STANDARD FOR SAFETY

Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements



SCC FOREWORD

National Standard of Canada

A National Standard of Canada is a standard developed by a Standards Council of Canada (SCC) accredited Standards Development Organization, in compliance with requirements and guidance set out by SCC. More information on National Standards of Canada can be found www.scc.ca.

SCC is a Crown corporation within the portfolio of Innovation, Science and Economic Development (ISED) Canada. With the goal of enhancing Canada's economic competitiveness and social well-being, SCC leads and facilitates the development and use of national and international standards. SCC also coordinates Canadian participation in standards development, and identifies strategies to advance Canadian standardization efforts.

Accreditation services are provided by SCC to various customers, including product certifiers, testing laboratories, and standards development organizations. A list of SCC programs and accredited bodies is publicly available at www.scc.ca.

UL Standard for Safety for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, ANSI/CAN/UL 2900-1

First Edition, Dated July 5, 2017

Summary of Topics

This revisions of ANSI/CAN/UL 2900-1, dated April 14, 2023, are issued to reflect the latest ANSI and SCC approval dates, and to include the following;

- ***Editorial Changes; [2.1](#), [6.7](#), [11.7](#), [15.5](#) and [15.6](#).***
- ***Addition of Inclusive Language; [3.30](#), [8.5](#)***
- ***Clarification of Product Documentation; [4.1](#)***
- ***Updated Versions of Reference Material; [2.1](#), [6.1](#), [11.5](#)***
- ***Addition of Paragraph Numbering; [7.1.4](#) and [7.1.5](#)***
- ***Clarification of Definitions and Term Usage; [3.14A](#), [8.3](#) and [8.8](#)***
- ***Clarification of Sensitive Data Documentation; [10.1](#) and [15.1](#)***
- ***Removal of Redundant Statement; [11.5](#)***
- ***Self-Reference Correction; [12.3](#) and [12.5](#)***
- ***Clarification of Structured Penetration Testing Requirements Documentation; [16.1](#) and [16.2](#)***
- ***Clarification of Software Composition, Static Source Code Analysis and Static Binary and Bytecode Analysis Requirements Documentation; [3.42A](#), Section [13](#), [14.2](#), [17.1](#), [17.2](#), [17.3](#), Section [18](#), [19.2](#) – [19.5](#), Section [A2](#), [Figure A1](#).***

Text that has been changed in any manner or impacted by ULSE's electronic publishing system is marked with a vertical line in the margin.

The new and revised requirements are substantially in accordance with Proposal(s) on this subject dated December 30, 2022.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means, electronic, mechanical photocopying, recording, or otherwise without prior permission of ULSE Inc. (ULSE).

ULSE provides this Standard "as is" without warranty of any kind, either expressed or implied, including but not limited to, the implied warranties of merchantability or fitness for any purpose.

In no event will ULSE be liable for any special, incidental, consequential, indirect or similar damages, including loss of profits, lost savings, loss of data, or any other damages arising out of the use of or the inability to use this Standard, even if ULSE or an authorized ULSE representative has been advised of the possibility of such damage. In no event shall ULSE's liability for any damage ever exceed the price paid for this Standard, regardless of the form of the claim.

Users of the electronic versions of UL's Standards for Safety agree to defend, indemnify, and hold ULSE harmless from and against any loss, expense, liability, damage, claim, or judgment (including reasonable attorney's fees) resulting from any error or deviation introduced while purchaser is storing an electronic Standard on the purchaser's computer system.



ANSI/UL 2900-1-2023



1

ANSI/CAN/UL 2900-1:2023

Standard for Software Cybersecurity for Network-Connectable Products,

Part 1: General Requirements

First Edition

July 5, 2017

This ANSI/UL Standard for Safety consists of the First Edition including revisions through April 14, 2023.

The most recent designation of ANSI/UL 2900-1 as an American National Standard (ANSI) occurred on April 14, 2023. ANSI approval for a standard does not include the Cover Page, Transmittal Pages, Title Page, Preface or SCC Foreword.

This standard has been designated as a National Standard of Canada (NSC) on April 14, 2023.

COPYRIGHT © 2023 ULSE INC.

No Text on This Page

CONTENTS

Preface	5
---------------	---

INTRODUCTION

1 Scope	9
2 Normative References	9
3 Glossary	11
4 Documentation Of Product, Product Design And Product Use	14
5 Product Design Documentation	15
6 Documentation for Product Use	15
7 Risk Controls	16
7.1 General	16
8 Access Control, User Authentication and User Authorization	17
9 Remote Communication	18
10 Sensitive Data	18
11 Product Management	19

RISK MANAGEMENT

12 Vendor Product Risk Management Process	20
---	----

I SOFTWARE COMPOSITION

13 Known Vulnerability Testing	21
13A Software Composition Analysis	22
14 Malware Testing	22
15 Malformed Input Testing	22
16 Structured Penetration Testing	23

SOFTWARE WEAKNESSES

17 Software Weakness Analysis	24
18 Static Source Code Analysis	24

SOFTWARE VULNERABILITIES

19 Static Binary and Bytecode Analysis	25
--	----

APPENDIX A (INFORMATIVE)

A1 Sources for Software Weaknesses	26
A2 Weaknesses and Vulnerabilities	26

APPENDIX B (INFORMATIVE)

B1 Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable Information	28
--	----

APPENDIX C (INFORMATIVE)

C1 Requirements for Security Functions	29
--	----

APPENDIX D (INFORMATIVE)

Preface

This is the First Edition of the ANSI/CAN/UL 2900-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements.

ULSE Inc. is accredited by the American National Standards Institute (ANSI) and the Standards Council of Canada (SCC) as a Standards Development Organization (SDO).

This Standard has been developed in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization.

This ANSI/CAN/UL 2900-1 Standard is under continuous maintenance, whereby each revision is approved in compliance with the requirements of ANSI and SCC for accreditation of a Standards Development Organization. In the event that no revisions are issued for a period of four years from the date of publication, action to revise, reaffirm, or withdraw the standard shall be initiated.

In Canada, there are two official languages, English and French. All safety warnings must be in French and English. Attention is drawn to the possibility that some Canadian authorities may require additional markings and/or installation instructions to be in both official languages.

Only metric SI units of measurement are used in this Standard. If a value for measurement is followed by a value in other units in parentheses, the second value may be approximate. The first stated value is the requirement.

Appendices [A](#), [B](#), [C](#), and [D](#), identified as informative, are for guidance and informational purposes only.

Comments or proposals for revisions on any part of the Standard may be submitted to ULSE at any time. Proposals should be submitted via a Proposal Request in ULSE's Collaborative Standards Development System (CSDS) at <http://csds.ul.com>.

Our Standards for Safety are copyrighted by ULSE Inc. Neither a printed nor electronic copy of a Standard should be altered in any way. All of our Standards and all copyrights, ownerships, and rights regarding those Standards shall remain the sole and exclusive property of ULSE Inc.

This Edition of the Standard has been formally approved by the Technical Committee (TC) on Software Cybersecurity for Network-Connectable Products: General Requirements, TC 2900-1.

This list represents the TC 2900-1 membership when the final text in this standard was balloted. Since that time, changes in the membership may have occurred.

TC 2900-1 Membership

Name	Representing	Interest Category	Region
Ahmadi, Mike	M Ahmadi	General	USA
Alvarez, Edison	Becton Dickinson	Producer	USA
Barker, Davis	Stanley Black & Decker	Producer	USA
Biggs, Douglas	UL Solutions	Testing & Stds Org	USA
Chevalier, Mathieu	Genetec	Producer	Quebec, Canada
Cosman, Eric	OIT Concepts LLC	Non voting member	USA
Datko, Joshua	Cryptotronics	General	USA
Dawson, Joe	EWA-Canada (an Intertek Co)	Testing & Stds Org	Newfoundland, Canada
Deskurakis, John	Carrier	Producer	USA
Dischert, Larry	Johnson Controls, Inc./Building Solutions North America	Commercial / Industrial User	USA
Dutta, Ashim	Eaton India Innovation Center	Producer	India
Fitzgerald, Brian	Food & Drug Administration	Government	USA
Fogleman, Greg	Department of Veterans Affairs	Government	USA
Garrett, Michael	Garrett Technologies Inc	General	USA
Garvy, Patrick	Honeywell	Producer	USA
Gatz, Stephen	Whirlpool Corp.	Producer	USA
Griffith, Steve	NEMA	Non-voting member	USA
Hicken, Arthur	PARASOFT	Testing & Stds Org	USA
Hornberger, Richard	Phoenix Contact Services Inc	Commercial / Industrial User	USA
Lee, Simon	U S Consumer Product Safety Commission	Non-voting member	USA
Leinonen, Juuso	ECRI	Supply Chain	USA
Li, Xiaodong	Lenovo (Beijing) Ltd	Producer	China
Martin, Robert	The Mitre Corporation	Commercial / Industrial User	USA
Maxey, Derek	Lockheed Martin Missiles & Fire Control	Supply Chain	USA
Mendoza, Ernesto	Signify North America Corporation	Producer	USA
Prince, Deborah R.	UL Standards & Engagement	TC Chair – Non-voting	USA
Rowland, Michael	IAEA	Government	Austria
Shkolnik, Moti	Firedome	Supply Chain	USA
Thayer, Rodney	Smithee Solutions LLC	General	USA
Tran, Phat	BC Safety Authority	Non-voting member	British Columbia, Canada
Treuthardt, Caroline	UL Standards & Engagement	TC Project Manager – Non-voting	USA
Vasserman, Eugene	Kansas State University	General	USA
Wang, Hui	CNCERT/CC	General	China
Wyman, Richard	CS 7 CONSULTING	General	USA

International Classification for Standards (ICS): 35.030, 35.110, 35.240.50

For information on ULSE Standards, visit <https://www.shopulstandards.com>, call toll free 1-888-853-3503 or email us at ClientService@shopULStandards.com.

■ This Standard is intended to be used for conformity assessment.

The intended primary application of this standard is stated in its scope. It is important to note that it remains the responsibility of the user of the standard to judge its suitability for this particular application.

CETTE NORME NATIONALE DU CANADA EST DISPONIBLE EN VERSIONS FRANÇAISE ET
ANGLAISE