



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

ULNORM.COM : Click to view the full PDF of UL 2900-1 2023



ANSI/UL 2900-1-2023



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.

ULNORM.COM : Click to view the full PDF of UL 2900-1 2022

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.

[ULNORM.COM](https://www.ulnorm.com) : Click to view the full PDF of UL 2900-1 2023



ANSI/UL 2900-1-2023

JULY 5, 2017
(Title Page Reprinted: April 14, 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

[ULNORM.COM](https://www.ulnorm.com) : Click to view the full PDF of UL 2900-1 2023

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
----	--	----

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
----	---	----