JOINT CANADA-UNITED STATES
NATIONAL STANDARD

ANSI/CAN/UL 2900-1:2026

STANDARD FOR SAFETY

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

ANSI/UL 2900-1-2026

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.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

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

Second Edition, Dated December 13, 2023

Summary of Topics

This revision of ANSI/CAN/UL 2900-1, dated June 29, 2026 includes incorporating inclusive language; 3.22 and 3.28.

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 revised requirements are substantially in accordance with Proposal(s) on this subject dated March 13, 2026.

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.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

ANSI/UL 2900-1-2026

DECEMBER 13, 2023
(Title Page Reprinted: June 29, 2026)

ANSI/CAN/UL 2900-1:2026

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

First EditionJuly, 2017

Second Edition

December 13, 2023

This ANSI/UL Standard for Safety consists of the Second Edition including revisions through June 29, 2026.

The most recent designation of ANSI/UL 2900-1 as an American National Standard (ANSI) occurred on June 29, 2026. 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 June 29, 2026.

© 2026 ULSE Inc. All rights reserved.

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

CONTENTS

Preface 5

INTRODUCTION

1 Scope 7
2 Normative References 7
3 Glossary 8
4 Documentation Of Product, Product Design And Product Use 12
5 Product Design Documentation 13
6 Documentation for Product Use 13
7 Risk Controls 14
7.1 General 14
8 Access Control, User Authentication and User Authorization 14
9 Remote Communication 16
10 Sensitive Data 16
11 Product Management 16

RISK MANAGEMENT

12 Vendor Product Risk Management Process 17

SOFTWARE COMPOSITION

13 Software Composition Analysis 19
14 Malware Testing 19
15 Malformed Input Testing 19
16 Structured Penetration Testing 21

SOFTWARE WEAKNESSES

17 Software Weakness Analysis 21

SOFTWARE VULNERABILITIES

18 Static Binary and Bytecode Analysis 22

ANNEX A (INFORMATIVE)

A1 Sources for Software Weaknesses 23
A2 Weaknesses and Vulnerabilities 23

ANNEX B (INFORMATIVE)

B1 Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable Information 25

ANNEX C (INFORMATIVE)

C1 Requirements for Security Functions 26

ANNEX D (INFORMATIVE)

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

No Text on This Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

Preface

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

ULSE 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.

Annexes 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 Interest	USA
Alvarez, Edison	Becton Dickinson	Producer	USA
Bhatt, Jatinkumar	Marmon Foodservice Technologies, Inc	Producer	USA
Callahan, Haley L.	UL Standards & Engagement	TC Chair – Non-voting	USA
Chevalier, Mathieu	Genetec	Producer	Canada
Chimalakonda, Sridhar	Indian Institute of Technology Tirupati	General Interest	India
Cosman, Eric	OIT Concepts LLC	Non-voting member	USA
Datko, Joshua	Cryptotronix	General Interest	USA

TC 2900-1 Membership Continued on Next Page

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

TC 2900-1 Membership Continued

Name	Representing	Interest Category	Region
Dawson, Joe	EWA-Canada (An Intertek Co)	Testing and Stds Org.	Canada
Dutta, Ashim	Eaton India Innovation Center	Producer	India
Fogleman, Greg	Department of Veterans Affairs	Government	USA
Friis, Paul	Whirlpool Corp	Producer	USA
Garine, Ramakishna	G Ramakrishna	General Interest	USA
Garrett, Michael	Garrett Technologies Inc	General Interest	USA
Griffith, Steve	National Electrical Manufacturers Association	Non-voting member	USA
Hicken, Arthur	Parasoft	Testing & Stds Org.	USA
Hornberger, Richard	Phoenix Contact Services Inc	Commercial / Industrial User	USA
Kirkland, Hannah	UL Standards & Engagement	TC Project Manager – Non-voting	Canada
Lee, Simon	U.S. Consumer Product Safety Commission	Non-voting member	USA
Li, Xiaodong	Lenovo (Beijing) Ltd	Producer	China
Martin, Robert	The Mitre Corporation	Commercial / Industrial User	USA
Maxey, Derek	Lockheed Martin Corporation	Supply Chain	USA
Mendoza, Ernesto	Signify North America Corporation	Producer	USA
Murray, James	J Murray	Consumer	USA
Rowland, Michael	IAEA	Government	Austria
Thayer, Rodney	Smithee Solutions LLC	General Interest	USA
Thieme, Andre	UL Solutions	Testing & Stds Org.	Germany
Tran, Phat	BC Safety Authority	Non-voting member	Canada
Vasserman, Eugene	Kansas State University	General Interest	USA
Wang, Hui	CNCERT/CC	General Interest	China
Yaghouby, Farid	FDA	Government	USA
Yang, Michael	Maple Armor	Producer	Canada
Yeruva, Sesha	Siemens Industry Inc	Producer	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

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.

INTRODUCTION

1 Scope

1.1 This standard applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware.

1.2 This standard describes:

a) Requirements regarding the software developer (vendor or other supply chain member) risk management process for their product.

b) Methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware.

c) Requirements regarding the presence of security risk controls in the architecture and design of a product.

1.3 This standard does not contain requirements regarding functional testing of a product. This means this standard contains no requirements to verify that the product functions as designed.

1.4 This standard does not contain requirements regarding the hardware contained in a product.

2 Normative References

2.1 All references are for the latest published version of the document, unless stated otherwise.

[1] IEEE 1149, *Standard for Test Access Port and Boundary-Scan Architecture*

[2] ITU-T X.1520, *Cybersecurity information exchange – Vulnerability/state exchange – Common vulnerabilities and exposures (CVE);*
retrievable from https://cve.mitre.org/

[3] ITU-T X.1521, *Cybersecurity information exchange – Vulnerability/state exchange – Common vulnerability scoring system (CVSS);*
retrievable from https://nvd.nist.gov/vuln-metrics/cvss

[4] ITU-T X.1524, *Cybersecurity information exchange – Vulnerability/state exchange – Common weakness enumeration (CWE)*

[5] ITU-T X.1525, *Cybersecurity information exchange – Vulnerability/state exchange – Common weakness scoring system (CWSS);*
retrievable from https://cwe.mitre.org/cwss

[6] ITU-T X.1544, *Cybersecurity information exchange – Event/incident/heuristics exchange – Common attack pattern enumeration and classification (CAPEC);*
retrievable from https://capec.mitre.org

[7] Common Weakness Risk Analysis Framework (CWRAF);
retrievable from https://cwe.mitre.org/cwraf/

[8] CWE/SANS Top 25 Most Dangerous Software Errors;
retrievable from cwe.mitre.org/top25

ULSE INC. COPYRIGHTED MATERIAL – NOT AUTHORIZED FOR FURTHER REPRODUCTION OR DISTRIBUTION WITHOUT PERMISSION FROM ULSE INC.