SmartSuite

Framework / Software Security / Other

ANSI/CAN/UL 2900-1, Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements (Edition 2)

UL 2900-1 (ANSI/CAN/UL 2900-1) is the ULSE standard for evaluating and testing the software of network-connectable products for vulnerabilities, software weaknesses and malware.



What it is

UL 2900-1, Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements (ANSI/CAN/UL 2900-1), is the UL Standards & Engagement (ULSE) standard that sets out how network-connectable products are evaluated and tested for vulnerabilities, software weaknesses and malware, what the software developer's risk management process must cover and which security risk controls the product's architecture and design must contain. Manufacturers of connected products, their software suppliers and the laboratories that test for them use it; Edition 2 was published on December 13, 2023 and revised on June 29, 2026.

Clause 1.1 states that the standard applies to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware. Clause 1.2 describes three things: requirements regarding the software developer's (vendor or other supply chain member) risk management process for their product; methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware; and requirements regarding the presence of security risk controls in the architecture and design of a product.

At a glance

PUBLISHER UL Standards & Engagement (ULSE)	TYPE Standard	VERSION Edition 2 (ANSI/CAN/UL 2900-1), published December 13, 2023; revised June 29, 2026
EFFECTIVE December 13, 2023 (Edition 2); revision June 29, 2026	DOMAIN Software Security	FAMILY Other
REGION United States and Canada	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: shopulstandards.com/ProductDetail.aspx?productId=UL2900-1

Why it matters

- **A fixed scope** Clause 1.1 names the subject: network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware.
- **Process and product together** Clause 1.2 pairs requirements on the vendor's risk management process with test methods for the product and controls in its design.
- **Supply chain included** Clause 1.2(a) applies to the software developer whether it is the vendor or another supply chain member, so component suppliers are inside the standard.
- **Clear exclusions** Clauses 1.3 and 1.4 keep functional testing and hardware out, which lets a cybersecurity evaluation run beside, not instead of, safety testing.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UL 2900-1

UL 2900-1 Requirement Library

Load the clause 1.2(a) to (c) subjects and the exclusions in clauses 1.3 and 1.4 as requirements with owners, implementation status and linked evidence per product.

Product Risk Management Record

Run the vendor risk management process of clause 1.2(a) as a register per product release: identified risks, assessment, treatment decisions and approvals.

Vulnerability, Weakness and Malware Test Evidence

Store laboratory and internal results from clause 1.2(b) evaluation and testing against each product version and route findings to remediation tasks.

Security Risk Controls in Design

Inventory the controls present in the architecture and design (clause 1.2(c)), with design review sign-offs and the risks each control addresses.

Supply Chain Member Oversight

Track each software supplier's obligations, risk management evidence and open findings in Third Party Risk Management, since clause 1.2(a) covers any supply chain member that develops the software.

Edition and Revision Tracking

Record the edition in force (Edition 2, revised June 29, 2026), open CSDS proposals and the Part 2 standards that apply, and reassess affected products when a revision is published.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · GDPR · IEC 62443 · ISO 27001:2022 · ISO 27002:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

UL 2900-1 Standard

Defines general requirements for software cybersecurity in network-connectable products.

shopulstandards.com/ProductDetail.aspx?productId=UL2900-1

UL Solutions Cybersecurity Services

UL Solutions testing, certification and advisory services for connected products, including its Cybersecurity Assurance Program.

ul.com/services/cybersecurity

UL 2900-2-1 catalog page (ULSE)

The catalog entry for Part 2-1 of the series, particular requirements for network connectable components of healthcare and wellness systems, with its scope and revision dates.

shopulstandards.com/ProductDetail.aspx?productId=UL2900-2-1

Explore UL Standards

Information on UL standards and how they are developed, from UL Standards & Engagement.

ulse.org/standards

Frequently asked questions

What does UL 2900-1 cover?

Clause 1.1 applies the standard to network-connectable products that shall be evaluated and tested for vulnerabilities, software weaknesses and malware. Clause 1.2 describes three subjects: requirements regarding the software developer's (vendor or other supply chain member) risk management process for the product, methods by which a product shall be evaluated and tested for the presence of vulnerabilities, software weaknesses and malware, and requirements regarding the presence of security risk controls in the architecture and design of a product.

What is the current edition of UL 2900-1, and when was it last revised?

Edition 2, designated ANSI/CAN/UL 2900-1, was published on December 13, 2023; Edition 1 is archived. The latest revision is dated June 29, 2026 and was approved by ANSI and by the Standards Council of Canada on the same date. ULSE's summary of topics says the revision incorporates inclusive language and amends definitions 3.22 and 3.28. A further CSDS proposal dated March 13, 2026 is listed on the catalog page, since ULSE keeps the standard under continuous maintenance.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

Does UL 2900-1 test whether a product works, or cover its hardware?

No. Clause 1.3 states that the standard does not contain requirements regarding functional testing of a product, meaning it contains no requirements to verify that the product functions as designed. Clause 1.4 states that it does not contain requirements regarding the hardware contained in a product. Functional and hardware safety are evaluated under other standards, several of which (UL 338, UL 1699, UL 1400-1, UL 2800-1-1) reference UL 2900-1 for the software cybersecurity part.

Who publishes UL 2900-1, and is the text free?

UL Standards & Engagement (ULSE), the standards development organization, publishes it; UL Solutions is the separate testing and certification company. The text is not free: the ULSE catalog lists it at $402.00 to $998.00 depending on format and subscription, in English and French. The catalog page itself shows the scope clauses, the edition and revision dates and the revision summary without charge.

How does UL 2900-1 relate to the other parts of the UL 2900 series?

Part 1 holds the general requirements, and Part 2 standards add particular requirements for a product family. UL 2900-2-1 (published September 1, 2017, last revised September 21, 2023) applies to the testing of network connectable components of healthcare systems, and UL 2900-2-3 (published January 31, 2020, last revised September 21, 2023) applies to the evaluation of security and life safety signaling system components. ULSE's catalog also lists UL 2900-1 as referenced by UL 2800-1-1, UL 338, UL 1699 and UL 1400-1.

License included / downloadable: No UL 2900-1 is published by UL Standards & Engagement (ULSE) and sold under a paid license (list price $402.00 to $998.00 on the ULSE catalog page, in English and French); the platform links to the catalog page, which carries the scope clauses and revision history free of charge.

Full framework page and mappings: smartsuite.com/frameworks/ul-2900-1-software-cybersecurity-network-connectable-products