WEB PINS FORM: STANDARDS ACTION PUBLIC REVIEW REQUEST

NOTE: This is a record of the submittal made on 2022-10-27 21:07:48 EDT. Adoptions of ISO or IEC standards require compliance with ANSI's Sales & Exploitation Policy.

PINS Standards Action Request Form Instructions

Accredited Standards Developer Information

Lynn First Name*	Barra Last Name*	Vice President, Standards Operations Title*		
INCITS/ITI Organization*		ITI (INCITS) Developer Acronym*		
700 K Street NW Suite 600 Address*		Washington City*	DC State*	20001 Submitter's Zip Code*
lbarra@itic.org Submitter's Email*		202-626-5739 Submitter's Phone*		Submitter's Fax

PINS Standard Action Request Entry form

Please enter your data for each standard into the fields below. Fields marked with an asterisk * are required. Once you have completed entering the data for the standard and you are ready to submit to ANSI, hit the **Submit to ANSI** button.

INCITS/ISO/IEC 27001:2022[202x]
Designation of Proposed Standard*

Information security, cybersecurity and privacy protection - Information security management systems - Requirements
Title of Standard*

Adopt identical ISO or IEC standard and revise current standard
Project Intent*

INCITS/ISO/IEC 27001:2013[R2019], INCITS/ISO/IEC 27001:2013/COR 1:2014[2019], INCITS/ISO/IEC 27001:2013/COR 2:2015[2018]
Supersedes or Affects

Adoption of this international standard is beneficial to the ICT Industry
Project Need*

ICT Industry
Identify Stakeholders*

Producer-Hardware, Producer-Software, Producer-General, Distributor, Service Provider, User, Consultants, Government, SDO and Consortia, Academic Institution, General Interest
Interest Categories*

ISO/IEC 27001:2022
Identify ISO or IEC standard to be adopted

(•) Yes ( ) No
Includes text from ISO or IEC standard?*

Metric
Unit of Measure*

( ) Yes (•) No
Revises a previous PINS submittal?*

Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. This document also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in this document are generic and are intended to be applicable to all organizations, regardless of type, size or nature. Excluding any of the requirements specified in Clauses 4 to 10 is not acceptable when an organization claims conformity to this document.
Scope Summary*

Notes

☑ Request an Announcement in Standards Action to Solicit New Consensus Body Members

* denotes required fields

<< Back
Standards Action Notification Date yyyy-mm-dd Save