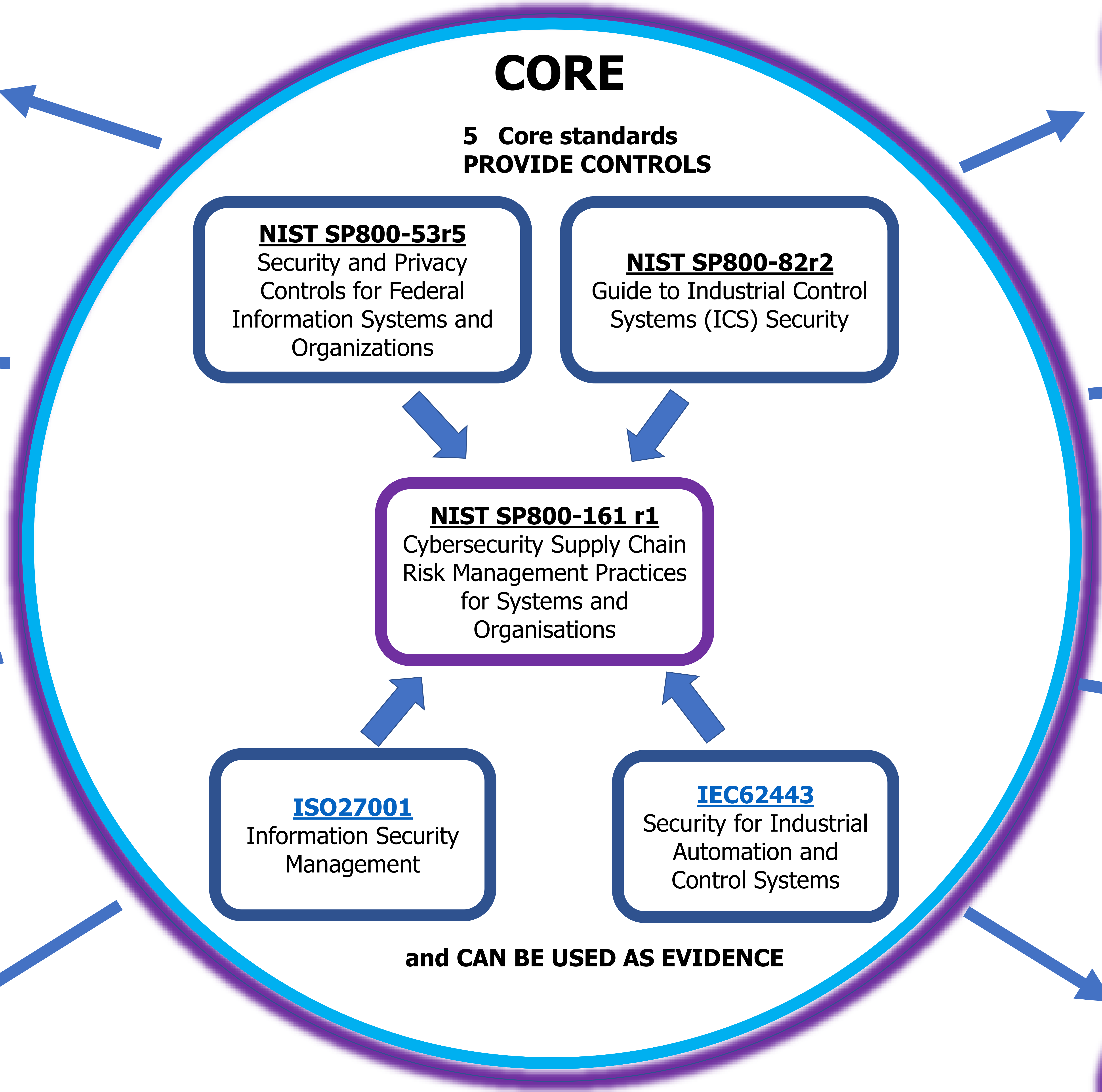
OT CNI Supply Chain Standards

Key Standards

Many of the standards identified as being most used are inter-related. NIST SP800-161 r1 can be used by organisations for identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations. Controls are provided by NIST SP800-53r5/B and where already existing these can also provide evidence of compliance. Similarly, proofs required for ISO27001 and IEC62443 can be used for NIST SP800-161 compliance. Many standards are available at no cost, those with licence fees are denoted in blue.



CORE

5 Core standards PROVIDE CONTROLS

NIST SP800-53r5
Security and Privacy Controls for Federal Information Systems and Organizations

NIST SP800-82r2
Guide to Industrial Control Systems (ICS) Security

NIST SP800-161 r1
Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations

ISO27001
Information Security Management

IEC62443
Security for Industrial Automation and Control Systems

and CAN BE USED AS EVIDENCE

SPACE SECTOR

NISTIR8270

ENERGY SECTOR

NERC CIP 013-1
IEC61850+IEC62351,
HSE OG86/Ofgem Guidance

TRANSPORT SECTOR

CENELEC TS 50701
DO-326/ED-202/ED-203
IMO MSC-FAL.1/Circ.3
SAE J3061 & SAE J3101

FACILITIES/ MANUFACTURING SECTOR

ETSI TS 303 645 V2.1
IoT Security Foundation Compliance Framework
Facility Cybersecurity Framework Best Practices –osti.gov

Please note that in the context of OT supply chain Emergency, Finance and Government are included in the IoT/BMS domain

FOOD SECTOR

IEC 61511 & IEC61508
PAS96

WATER SECTOR

ANSI/AWWA G430-09/"Security Practices for Operations and Management"

CHEMICAL SECTOR

Chemical Facility Anti-Terrorism Standards
HSE OG86

HEALTH SECTOR

MHRA/EMA GLP & GMP
MHRA IoMT Guidance

ASSURANCE

UK NCSC Cyber Assessment Framework (A4 Supply Chain)
ISO/IEC 15408-1:2009 – Evaluation Techniques
ISO/IEC 17025:2017 – Test Lab Standards
National Defense Industrial Association (NDIA) Engineering for System Assurance
OWASP Software Assurance Maturity Model (SAMM) Version 2.0
SAFECode, Software Integrity Controls
SSAE 18 SOC2/SOC 3 Reports
NIST NISTIR7622 – Notional Supply Chain risk management practices

Produced by the NCSC ICS Community of Interest Supply Chain Expert Group (SCEG)

OT Supply Chain Cyber Security Assurance Standards for Critical National Infrastructure

An Infographic Introduction and Guide

Draft Version 1.7, 22nd June 2023

This Infographic and set of supporting materials has been created by the NCSC ICS COI Supply Chain Expert Group (SCEG) to assist supplier and customer organisations to understand which reference standards used in supply chain cyber security assurance are seen as the most important for all sectors and also which are the most relevant for specific sectors. The priority and importance has been drawn from our own experience in practice and recognises that some national standards have international influence in the supply chain. We have not covered defence or civil nuclear because of the special requirements of these sectors.

This is a work in progress and is still under development. It has been made available as early as possible in the hope that it is of immediate value, and to ask for comments and feedback on how it can be enhanced and improved. The next version will have more details on the different aspects of 'combined' sectors such as energy and transportation where there are more specific standards for different parts of the sector (e.g. road, rail, maritime, aviation).   Comments can be sent to paul.dorey@rhul.ac.uk. **and to https://forms.gle/AczjgMVQ3FvHD9jb8**

NCSC ICS Community of Interest Supply Chain Expert Group (SCEG)

The SCEG is a volunteer initiative to progress multiple-sector wide approaches to the challenge of overseeing, managing and influencing the cyber security of supply chains to critical infrastructure services. Co-Led by Paul Dorey (Royal Holloway) and Tania Wallis (Glasgow University) the group has membership of experienced experts from different sectors and parts of the supply chain.

Standards and Guidance Infographic - SCEG Participants:

Principal Author: Richard Smith, De Montfort University
Contributors: Hugh Boyes, Jennifer Burke, Paul Dorey, John French, Chris McGookin, John Parsons, Paul Richardson, John Thornley, Richard Thomas, Tania Wallis
Reviewers: Roger Dias, Jane Goble, Michael Jacks, Clare McBrearty, Nikita Johnson, Tom Padden, Emma Taylor, Colin Topping, Lydia Walker, Kevin Wood, John Wright