ISO/IEC JTC 1/SC 27/WG 4 N 2768

ISO/IEC JTC 1/SC 27/WG 4

Security controls and services

Convenorship: ILNAS (Luxembourg)

Document type:	National Body Contribution
Title:	NB proposal SP Connected devices - Proposal by US NB for a study period on Security and Privacy Baseline Controls for Connected Devices
Status:	This document is distributed for information and consideration at the 27th meeting of ISO/IEC JTC 1/SC 27/WG 4 to be held in Gjøvik, Norway, from 2018-09-30 to 2018-10-04.
Date of document:	2018-09-07
Source:	US NB
Expected action:	ACT
Action due date:	2018-10-04
No. of pages:	1 + 4
Email of convenor:	amsenga@gmail.com
Committee URL:	https://isotc.iso.org/livelink/livelink/open/jtc1sc27wg4

ISO/IEC JTC 1/SC 27 N18885

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology -- Security techniques

Secretariat: DIN, Germany

DOC TYPE:	**national body contribution**
TITLE:	**US National Body contribution on Proposal to Request a new WG 4 Study Period on Security and Privacy Baseline Controls for Connected Devices**
SOURCE:	**ANSI, National Body of United States**
DATE:	**2018-09-07**
PROJECT:	
STATUS:	**This document has been forwarded to SC 27/WG 4 for consideration at its 27th meeting in Gjøvik, Norway, 2018-09-30/10-04. It is being circulated within SC 27 for information.**
ACTION ID:	**ACT/INFO**
DUE DATE:	
DISTRIBUTION:	**P-, L- and O-Members** **A. Wolf, Acting SC 27 Chairman** **M. De Soete, SC 27 Vice-Chair** **E. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors**
MEDIUM:	**http://isotc.iso.org/livelink/livelink/open/jtc1sc27**
NO. OF PAGES:	**1 + 3**

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., A DIN-Platz, Burggrafenstr. 6, D-10787 Berlin [postal D-10772], Germany,
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-4-2652; E-mail: krystyna.passia@din.de
HTTP://www.din.de/go/jtc1sc27

US Proposal to Request a WG 4 Study Period on Security and Privacy Baseline Controls for Connected Devices

While the work on ISO/IEC 27030 has started progressing, there has been an increasing demand for context-specific security and/or privacy baseline controls. With this in mind, we believe that a study period to develop the text for this area, taking into account the trends in the industry, would be helpful. This study would be done as a complementary effort to the work on ISO/IEC 27030 and should not be done in isolation of ISO/IEC 27030.

Reviews done by various government organizations have found that security and privacy baselines and protections for connected devices are lacking and that these protections need to be put in place. Reports such as the one published by the Dept for Digital, Culture, Media & Sport: Secure by Design: Improving the cyber security of consumer Internet of Things Report[1] and ENISA's report Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures[2] call for the need for security baselines and code of practices for ensuring the security of connected devices and the systems they interact with. These reports are not limited to just the European Union, there is also a growing concern in Japan, the US and other countries around the world.

While there are efforts started within the standards world, in particular ISO/IEC JTC 1/SC 27 with ISO/IEC 27030 and ISO/IEC JTC 1/SC 41 (as well as discussions about new work in ETSI TC Cyber and CEN/CENELEC JTC 13), we believe that there needs to be further work to harmonize these efforts related to the need for security and/or privacy baselines. The work on ISO/IEC 27030 has a very broad scope: "This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions." The work on this document touches on very important aspects of IoT Security and Privacy, but additional focus is needed on security and privacy baseline controls. We believe that by leveraging the existing work that has been done on ISO/IEC 27030 and some of the trustworthiness work in ISO/IEC JTC 1/SC 41, the concerns around security and/or privacy baseline controls can be addressed.

What is not clear is the best approach for addressing this. While it is clear that controls are within scope of ISO/IEC 27030, it seems that the document is covering a lot of area including the risks of IoT, principles to be used, security management processes and a life cycle. It may be more effective for the controls and security and/or privacy baseline aspects of IoT security and other connected devices to be broken out into another document, or the existing document to be split into multiple parts with one of those parts being security and/or privacy baseline controls. There may also be other options available. What is clear is that further investigation is needed to identify common factors in the reports that have been produced. These could be harmonized in an International Standard so that there is consistency among the various global regulations, legislation and recommendations. To begin this investigation, we have already identified several reports and organizations that are starting work on security and/or privacy baselines, controls or the possibility of requiring certifications and they are:

1. UK Dept for Digital, Culture, Media & Sport: Secure by Design: Improving the cyber security of consumer Internet of Things Report:

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

[2] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

2. ENISA - Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
3. US Senate: Internet of Things (IoT) Cybersecurity Improvement Act of 2017 : https://www.congress.gov/bill/115th-congress/senate-bill/1691/text
4. METI: The Cyber/Physical Security Framework (Draft)
5. EU Parliament: Proposed ITRE amendment 577
6. NIST Cybersecurity for IoT (including NISTIR 8200 *Status of International Cybersecurity Standardization for Internet of Things (IoT)*)
7. CEN/CENLEC SG 13
8. US Report to the President on Enhancing Resilience Against Botnets https://www.commerce.gov/page/report-president-enhancing-resilience-against-botnets

We believe that a study period to identify these commonalities and put together a draft for an International Standard that will address the security and/or privacy baseline controls for IoT systems would be the most effective way forward. This study period can be done in parallel with the existing projects and take into consideration the existing projects. One outcome of this study period could be a determination of the most appropriate way to interact with ISO/IEC 27030. With this in mind we are recommending the following Study Period and Terms of Reference:

1. Proposal

Establish a 6-month Study Period on connected devices Security and/or Privacy baseline controls

2. Motivation and Scope

As there is an increasing number of reports from government and other organizations recommending legislation and regulations for security and/or privacy baseline controls for connected devices, there is a desire to drive harmonization around the commonalities of these baseline controls. While work is beginning on the security and privacy of IoT, there is still a large landscape to cover relating to connected devices.

We therefore propose this Study Period in order to:

1. Identify the commonalties in various global security and/or baseline reports, proposed legislation and draft recommendations.

2. Identify additional controls needed in the area of connected devices and IoT security and/or privacy

3. Examine the existing IoT security and privacy work in ISO/IEC JTC 1/SC 27 and ISO/IEC JTC 1/SC 41 to avoid duplication.

3. Activities

The Study Period is requested to:

1) Consider the relationship of ISO/IEC 27030's scope to this Study Period;

2) Collect information from SC27 experts on relevant reports, draft legislation, regulations and existing work on connected devices and IoT Security and/or privacy baseline controls;

3) Consider effects of pre and post-market requirements;

4) Invite other National Bodies, Liaisons Organizations and other JTC1 SCs concerned by the subject to submit suggested topics and/or feedback;

5) Ensure representation from all SC 27 WGs and SWG-T as required, to participate in the study;

6) Hold virtual study period meetings to flush out ideas, issues, and critical success factors;

4. Deliverables

a. Text for security and/or privacy baseline controls for connected devices
b. Report and recommendations
c. If appropriate, NWIP and Draft document

The U.S. is also prepared to offer Laura Lindsay as a Rapporteur.