|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| D:\usr\campos\TSB-Reference\Logos\ITU\sigleITU.gif | INTERNATIONAL TELECOMMUNICATION UNION  **TELECOMMUNICATION STANDARDIZATION SECTOR**  STUDY PERIOD 2017-2020 | | | JCA-AHF-441 | |
|  |  | | | **JCA-AHF** | |
|  |  | | | **Original: English** | |
| **Question(s):** | | N/A | Virtual Geneva, 2 September 2021 | | |
| **DOCUMENT** | | | | | |
| **Source:** | | Brian Copsey | | | |
| **Title:** | | Cyber Security and potential issues for Persons with Disabilities and specific needs: an overview | | | |
| **Purpose:** | | Discussion | | | |
| **Contact:** | | Brian Copsey CCC UK | | | Tel: +44 7860 300552 Fax:  E-mail: BC@copsey-comms.com |

|  |  |
| --- | --- |
| **Keywords:** | Cyber Security; |
| **Abstract:** | Cyber Security and potential issues for Persons with Disabilities and specific needs |

# Cyber Security and potential issues for Persons with Disabilities and specific needs: an overview

*The following comments and views are my own and should not be associated with any organisations I normally represent at ITU.*

Whilst this document focuses on items raised during the draft EU work, similar regulation/standardisation is either in place (Brazil) or under consideration FCC and UK

This is an extremely difficult subject to fully express but I hope to have provided enough examples to start a debate and consider the next steps, (if any) and I seek your help in achieving this

## Background

To date cyber security regulation and standardisation has almost exclusively focused on “networks” i.e. telephone both wired and wireless plus large computer systems used by industry, within the EU an issue on a toy doll was raised in about 2014.

Karla dolls use wireless to allow parents to view, hear and talk to the child. It was considered that if someone else where able to hack into the dolls facilities they could groom the child or put the child in a dangerous position with an unauthorised adult.

Following debate within the EU it was decided to investigate the issue and this resulted in sections being written into the Radio Equipment Directive 2014[[1]](#footnote-1) (which is for placing radio devices onto the EU market) but not activated.

Following various reports and consultations it was decided action was necessary to “*ensure that the concerned radio equipment protect the user from elements of cyber security*” risks and activate those sections via a Delegated Act[[2]](#footnote-2) which is in the final stages of preparation and will most probably come into force late 2021 or early 2022 with a 30 month window for the standards to be written and industry to then show compliance.

## Delegated Act

References a range of issues for radio devices which can be connected directly or indirectly connected to the internet, it currently includes 5G

The Delegated Act requires “Devices” to support

*the protection of personal data and privacy of users and of subscribers of radio equipment and the protection from fraud may be enhanced by particular features of radio equipment. Radio equipment should therefore in appropriate cases be designed in such a way that it supports those features*.

Also provide secure uploads for both security and equipment software updates

Whilst there is a lot more detail available the overview above provide a background for my following comments

## Issues which require consideration

General

From the past 18 months discussion within ETSI-CENELEC-EC there is a conundrum between defining facilities to ensure a secure radio device and how Persons with Disabilities and specific needs will not be digitally disadvantaged

Dependant on age and specific disability the following issues could affect a person’s ability to use and update a device

**Passwords**: a basic security tool, the proposal to prevent universal passwords is reasonable until you consider human memory especially with those who are not computer literate. If a manufacturer cannot have a universal password they can not help access a locked device

Whilst not currently mandated the trend is for ever longer and complex passwords in excess of 8 characters. If complex passwords are required every time you require to use a device then a wide range of people will undoubtedly hesitate before using that device or be unable to access it at some point

Add to this the plethora of passwords an individual has to have which will soon include items such as washing machines and fridges. In my case I have a list which is shared with my daughters so that in case of illness, death or dementia they can access my devices as I believe I am not alone in having most important information stored on my PCs

Questions:

1. How do we identify a level of password(s) which can be used Persons with Disabilities and specific needs?
2. Should there be a facility for no passwords on devices?
3. Are fingerprints or eye recognition appropriate?
4. How do we express this issue to those putting in place legislation and standardisation?

**Software Updates:** manufacturers will be required to provide security updates for the lifetime of the device as well as software updates. Such updates must be secure to prevent hackers attaching bugs to the update. Such updates are unlikely to be fully automatic and require users to validate via their device of possibly a computer or mobile phone.

Questions:

1. Which form of validation is suitable
2. Do we have other systems which would be usable?

**Personal data and Fraud:** Devices must secure personal data and prevent fraud, similar considerations as to passwords and updates need addressing

**5G**: *5G will potentially affect almost every aspect of Union citizens' life. All 5G equipment is expected to be internet-connected and such equipment should support the deployment of secure 5G networks. It is consequently of the utmost importance to ensure that the networks where 5G equipment operate are not sufficiently secure because of certain classes or categories of radio equipment which are placed on the Union market.*

Whilst we are still seeking to fully understand the requirements of the EC in this area it is likely to include increase security access and possibly consideration of apps being loaded onto a handset by either the manufacturer or user

Many handsets are already difficult to access and “time out” frequently and if in addition high level security is also required for each app then the access problem is exponential

# Medical devices

Currently devices coming under the EC Medical Directive are exempt ***BUT*** many devices such as hearing aids, heart monitors and cochlear implants also come under the Radio Equipment Directive and are subject to compliance with it. As the Medical Directive already has very strict security requirements we are in danger of both double testing and conflicting requirements. We have requested clarity on this issue but have not received it.

Accessories not coming under the Medical Directive but connecting to Medical Devices will not be covered by this exemption

Question:

1. Should this issue be identified in any subsequent work and clear recommendations made

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0053&rid=7 [↑](#footnote-ref-1)
2. file:///C:/Users/BC/Dropbox/Documents/ITU%20Disability/JCA-AHF/August%202021/software%20clarifications%20-%20EN.pdf [↑](#footnote-ref-2)