INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

ITS – LS 7 – E

Original: English

WG(s): Geneva, 10 March 2017

LS

Source: Collaboration on ITS Communication Standards (CITS)

Title: LS on request for input on automotive cybersecurity and OTA issues

Purpose: Discussion

LIAISON STATEMENT

For action to: UNECE Task Force on cybersecurity and OTA issues (CS/OTA)

For comment to: -

For information to: ITU-T SG 17

Approval: CITS Meeting (Geneva, 10 March 2017)

Deadline: -

Contact: T. Russell Shields
CITS Co-Chair
E-mail: trs@ygomi.com

Contact: Koji Nakao
NICT
Japan
E-mail: ko-nakao@nict.go.jp

Keywords: Cybersecurity; OTA; standards;

Abstract: The Collaboration on ITS Communication Standards is requesting input on standards gaps in the area of automotive and ITS cybersecurity.

ITU is the United Nations specialized agency for information and communication technologies (ICTs). It allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies seamlessly interconnect, and strives to improve access to ICTs to underserved communities worldwide.

ITU's membership is comprised of 193 Member States, over 700 Sector Members and Associates from industry, international, and regional organizations, and 140 Academic Members.

ITU is organizing a collaboration activity on communication standards for intelligent transportation systems – Collaboration on ITS Communication Standards (http://itu.int/go/ITScomms) – which aims at providing a forum to promote an internationally accepted, globally harmonized set of standards.

The Collaboration is also a venue for information exchange between ITU study groups and other organizations active in the field of ITS communication standards.

Within ITU's standardization sector, Study Group 17 (http://itu.int/go/tsg17) is the responsible group for cybersecurity; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security

of applications and services for the Internet of Things (IoT), ITS (including co-operative ITS), smart grid, smartphones, software defined networking (SDN), web services, big data analytics, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

Study Group 17 currently has two work items in the area of ITS cybersecurity:

- X.1373 (ex. X.itssec-1): *Secure software update capability for intelligent transportation system communication devices*. This draft Recommendation describes secure software update procedures between software update server and vehicles with appropriate security controls. This Recommendation can be practically utilized by car manufactures and ITS-related industries as a set of standard capabilities for best practices. The draft was determined in September 2016, and is now awaiting comments from the membership (TAP consultation process) to be approved by SG17 in its Geneva, 22-30 March 2017 meeting.

- X.itssec-2: *Security guidelines for V2X communication systems*. This Recommendation aims at providing security guidelines for V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-Infrastructure) and/or V2N (Vehicle-to-Nomadic Device) communication systems. This work item is under development, and planned to be completed by October 2017.

The next meeting of Study Group 17 will take place in Geneva, 22-30 March 2017. This will be the first meeting of the Study Period, and lay out the ITU cybersecurity standardization activities for the time 2017-2020.

To offer guidance to Study Group 17, the Collaboration on ITS Communication Standards calls for input from the UNECE Task Force on cybersecurity and OTA issues (CS/OTA) on any standards gaps identified in the area of automotive and ITS cybersecurity that would benefit from international standards.

_____