EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 4

ANNEX

to the

Commission Delegated Regulation

supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TABLE OF CONTENTS

ANNEX IV

1. C-ITS SECURITY POLICY

1.1. Definitions and acronyms

EU CCMS	European Union C-ITS security credential management system
CAM	cooperative awareness message
CP	certificate policy
DENM	decentralised environmental notification message
ISMS	information security management system
IVIM	infrastructure-to-vehicle information message
SPATEM	signal phase and timing extended message
SREM	signal request extended message
SSEM	signal request status extended message

1.2. Definitions

availability	being accessible and usable on demand by an authorised entity (ISO 27000) [2]
C-ITS infrastructure	system of facilities, equipment and applications needed for the operation of an organisation that provides C-ITS services related to fixed C-ITS stations.
C-ITS stakeholders	individual, group or organisation with a role and responsibility in the C-ITS network
confidential information	information that is not to be made available or disclosed to unauthorised individuals, entities or processes (ISO 27000) [2]
information security	preservation of the confidentiality, integrity and availability of information (ISO 27000) [2]
information security incident	an unwanted or unexpected information security event, or series of events, that has a significant probability of compromising business operations and threatening information security
integrity	property of accuracy and completeness (ISO 27000) [2]
local dynamic	an in-vehicle C-ITS station's dynamically updated repository of data relating to local driving

map (LDM)	conditions; it includes information received from on-board sensors and from CAM and DENM messages (ETSI TR 102 893) [5]
protocol control	The protocol control assets select an appropriate message transfer protocol for an outgoing message request and send the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the C-ITS station and passed to the relevant functional asset for further processing (ETSI TR 102 893) [5]

1.3. Strategy for information security

1.3.1. Information security management system (ISMS)

(1) Each C-ITS station operator shall operate an ISMS in accordance with ISO/IEC 27001 and with the constraints and additional requirements laid down in this section.

(2) Each C-ITS station operator shall determine external and internal issues relevant to C-ITS, including:

- COM(2016) 766 final [10];
- the GDPR [6].

(3) Each C-ITS station operator shall determine parties that are relevant to the ISMS and their requirements, including all C-ITS stakeholders.

(4) The ISMS scope shall include all the operated C-ITS stations and all other information-processing systems that process C-ITS data in the form of C-ITS messages that comply with the following standards:

- CAM [7]
- DENM [8]
- IVIM [9]
- SPATEM [9]
- MAPEM [9]
- SSEM [9]
- SREM [9]

(5) Each C-ITS station operator shall ensure that its information security policy is consistent with this policy.

(6) Each C-ITS station operator shall ensure that its information-security objectives include and are consistent with the security objectives and high-level requirements in this policy.

(7) C-ITS station operators shall classify the information referred to in section 1.4.

(8) C-ITS station operators shall apply an information security risk assessment process as set out in section 1.5 at planned intervals or when significant changes are proposed or occur.

(9) C-ITS station operators and/or C-ITS station manufacturers shall determine requirements for mitigating security risks identified in the information security risk assessment process, in line with section 1.6.

(10) C-ITS station manufacturers shall design, develop and assess C-ITS stations and other information processing systems so as to ensure that they meet applicable requirements.

(11) C-ITS station operators shall operate C-ITS stations and all other information-processing systems that implement appropriate information security risk treatment controls in line with section 1.6.

1.4. Information classification

This section lays down the minimum requirements for information classification. This does not prevent any C-ITS stakeholder from applying more stringent requirements.

(12) C-ITS station operators shall classify handled information, whereby a security category can be represented as:

Security Category information = {(confidentiality, impact), (integrity, impact), (availability, impact)};

(13) C-ITS stakeholders shall classify managed information, whereby a security category system can be represented as:

Security Category information system = {(confidentiality, impact), (integrity, impact), (availability, impact)};

(14) The acceptable values for potential impact are low, moderate and high, as summarised Table **1**.

Table 1 Potential impact definitions for each security objective of confidentiality, integrity and availability

	Potential impact		
Security objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.
Integrity Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.

	Potential impact		
Availability Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.

(15) The following information classification impact types shall be considered in terms of the degree of damage or costs to the C-ITS service and C-ITS stakeholders caused by an information security incident:

- road safety — where the impact places road users at imminent risk of injury;
- safety — where the impact places any of the C-ITS stakeholders at imminent risk of injury;
- operational impacts — where the impact is substantially negative for road traffic efficiency, or other societal impact such as environmental footprint and organised crime;
- legal — where the impact results in significant legal and/or regulatory compliance action against one or more of the C-ITS stakeholders;
- financial — where the impact results in direct or indirect monetary costs for one or more of the C-ITS stakeholders;
- privacy – the GDPR having both legal and financial impact;
- reputation — where the impact results in reputational damage for one or more C-ITS stakeholders and/or the C-ITS network, e.g. adverse press coverage and/or major political pressure on a national or international scale.

(16) C-ITS stakeholders shall respect the following minimum impact values for the information handled:

Table 2: Impacts

	Information originated by fixed C-ITS stations	**Information originated by mobile C-ITS stations**
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low personal data contained in any of the three messages: moderate
Integrity	CAM: moderate	CAM: moderate

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
	DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

1.5. Risk assessment

1.5.1. General

(17) Risk assessment shall be periodically conducted in line with ISO/IEC 27005. It shall include appropriate documentation of:

- the scope of the risk assessment, i.e. the system being assessed and its boundaries and system purpose, and the information that is handled;
- the security risk criteria;
- risk assessment, including identification, analysis and evaluation.

1.5.2. Security risk criteria

(18) Risk evaluation criteria shall be determined considering the following aspects:

- the strategic value of the C-ITS service and C-ITS network to all C-ITS stakeholders;
- the strategic value of the C-ITS service and C-ITS network to the C-ITS station operator of the service;
- the consequences for the reputation of the C-ITS network;
- legal and regulatory requirements and contractual obligations.

(19) Risk impact criteria shall be determined in the light of the information classification impact types referred to in section 1.4.

(20) Risk acceptance criteria shall include the identification of risk levels that are unacceptable for the C-ITS service and C-ITS stakeholders, by impact type.

1.5.2.1. Risk identification

(21) Risks shall be identified in accordance with ISO/IEC 27005. The following minimum requirements shall apply:

- the main assets to be protected are C-ITS messages as referred to in section 1.3.1;

- supporting assets should be identified, including:
    - information used for C-ITS messages (e.g. local dynamic map, time, protocol control, etc.);
    - C-ITS stations and their software, configuration data and associated communication channels;
    - central C-ITS control assets;
    - every entity within the EU CCMS;
- threats to those assets, and their sources, shall be identified;
- existing and planned controls shall be identified;
- vulnerabilities that can be exploited by threats to cause harm to assets or to the C-ITS stakeholders shall be identified and described as incident scenarios;
- the possible consequences of security incidents on the assets shall be identified on the basis of the information classification.

1.5.2.2. Risk analysis

(22) The following minimum requirements apply to risk analysis:

- the impact of the identified information security incidents on the C-ITS service and the C-ITS stakeholders shall be assessed on the basis of the information and information system security category, using at least the three levels set out in section 1.4;
- the levels of impact shall be identified for:
    - the total existing C-ITS network/services; and
    - an individual C-ITS stakeholder/organisational entity;
- the highest level shall be taken as total impact;
- the likelihood of the identified incident scenarios shall be assessed using at least the following three levels:
    - unlikely (value 1) – the incident scenario is unlikely to occur / difficult to realise or the motivation for an attacker is very low;
    - possible (value 2) – the incident scenario may occur/ is possible to realise or the motivation for an attacker is reasonable;
    - likely (value 3) – the incident scenario is likely to occur / easy to realise and the motivation for an attacker is high;
- the levels of risk shall be determined for all identified incident scenarios on the basis of the product of impact and likelihood, resulting in at least the following risk levels: low (values 1,2), moderate (values 3,4) and high (values 6,9), defined as follows:

Table 3: Risk levels

Risk levels as product of impact and likelihood		Likelihood		
		unlikely (1)	**possible (2)**	**likely (3)**
Impact	**low (1)**	low (1)	low (2)	moderate (3)
	moderate (2)	low (2)	moderate (4)	high (6)
	high (3)	moderate (3)	high (6)	high (9)

1.5.2.3. Risk evaluation

(23) Levels of risk shall be compared against risk evaluation criteria and risk acceptance criteria to determine what risks shall be subject to treatment. At least moderate- or high-level risks applicable to the C-ITS service and C-ITS network shall be treated, in line with section 1.6.

1.6. Risk treatment

1.6.1. General

(24) Risks shall be treated in one of the following ways:

- risk modification by using controls identified in section 1.6.2 or 1.6.3, so that the residual risk can be reassessed as being acceptable;
- risk retention (where the level of risk meets the risk acceptance criteria);
- risk avoidance.

(25) Risk sharing or transfer is not allowed for risks to the C-ITS network.

(26) Risk treatment shall be documented, including:

- the statement of applicability in line with ISO 27001, which sets out the necessary controls and determines:
  - the residual likelihood of occurrence;
  - the residual severity of impact;
  - the residual risk level;
- the reasons for risk retention or avoidance.

1.6.2. Controls for C-ITS stations

1.6.2.1. Generic controls

(27) C-ITS stations shall implement appropriate countermeasures to modify risk, in line with section 1.6.1. Those countermeasures shall implement generic controls as defined in ISO/IEC 27001 and ISO/IEC 27002.

1.6.2.2. Controls for communication between C-ITS stations

(28) The following minimum mandatory controls shall be implemented on the sender side:

Table 4: Controls on the sender side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality	-	The personal data contained in messages shall be secured using an adequate AT change procedure to ensure a level of security adequate to the risk of re-identification of drivers based on their broadcasted data. Therefore, C-ITS stations shall change ATs adequately when sending messages and shall not re-use ATs after a change, except in cases of non-average[1] driver behaviour.
Integrity	All messages shall be signed in accordance with TS 103 097 [14].	All messages shall be signed in accordance with TS 103 097 [14].
Availability	-	-

(29) The following minimum mandatory controls shall be implemented on the receiver side:

Table 5: Controls on the receiver side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality		Received personal data should be retained for as short a time as possible for business purposes, with a **maximum retention of five minutes** for raw and identifiable data-elements. A received CAM or SRM shall not be forwarded/broadcast. A received DENM may be forwarded/broadcast only within a limited geographical area.
Integrity	The integrity of all messages used by ITS applications shall be validated in accordance with TS 103 097 [14].	The integrity of all messages used by ITS applications shall be validated in accordance with TS 103 097 [14].
Availability	-	A received SRM shall be processed and produce an SSM broadcast to the originator of the SRM.

(30) To support the security requirements of confidentiality, integrity and availability set out in the tables above, all C-ITS stations (mobile C-ITS stations (including vehicle C-ITS stations) and fixed C-ITS stations) shall be assessed and certified using security assessment criteria as specified in the 'common criteria' / ISO 15408[2]. Due to the different features of the different types of C-ITS station and different location privacy requirements, different protection profiles may be defined.

[1] The definition of average driving behaviour shall be based on relevant statistical analysis of the driving behaviour in the European Union, e.g. based on data from the German Aerospace Centre (DLR).

[2] 'Common criteria' portal: http://www.commoncriteriaportal.org/cc/

(31) All protection profiles and related documents applicable for the security certification of the C-ITS stations shall be evaluated, validated and certified in line with ISO 15408, applying the *Mutual Recognition Agreement of information technology security evaluation certificates* of the Senior Officials Group on Information Systems Security (SOG-IS)[3], or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity framework. In the development of such protection profiles, the scope of the security certification of the C-ITS station may be defined by the manufacturer, subject to assessment and approval of the CPA and a SOG-IS conformity assessment body or at least equivalent as described in the next paragraph.

(32) Given the importance of maintaining the highest possible security level, security certificates for C-ITS stations shall be issued under the common criteria certification scheme (ISO 15408) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS agreement, or issued by a conformity assessment body accredited by a national cybersecurity certification authority of a Member State. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

1.6.2.3. Controls for C-ITS stations as an end-entity

(33) C-ITS stations shall comply with the certificate policy [1] according to their role as an EU CCMS end-entity.

1.6.3. Controls for EU CCMS participants

(34) EU CCMS participants shall comply with the certificate policy [1] according to their role in the EU CCMS.

1.7. Compliance with this security policy

(35) C-ITS station operators shall periodically request and obtain certification for compliance with this policy following the guidelines for an ISO 27001 audit in [12].

(36) The auditing body shall be accredited and certified by a member of European Accreditation. It shall fulfil the requirements of [11].

(37) With the objective of obtaining certification, C-ITS station operators shall generate and maintain documents addressing the requirements on documented information in [3], clause 7.5. In particular, C-ITS station operators shall generate and maintain the following documents related to the ISMS:

- scope of the ISMS (section 1.3.1 and [3], clause 4.3);
- information security policy and objectives (section 1.3.1 and [3], clauses 5.2 and 6.2);
- risk assessment and risk treatment methodology details (section 1.5 and [3], clause 6.1.2);

[3] In the road transport sector, SOG-IS has already been involved in the smart tachograph security certification, for example. The SOG-IS Agreement is currently the only scheme in Europe that can support the harmonisation of security certification of electronic products. At this stage, SOG-IS supports only the 'common criteria' process, so the C-ITS stations must be assessed and certified in line with the 'common criteria'; see https://www.sogis.org/

- risk assessment report (section 1.5 and [3], clause 8.2);
- statement of applicability (section 1.6 and [3], clause 6.1.3d);
- risk treatment plan (section 1.6 and [3], clauses 6.1.3e and 8.3);
- documents required for the implementation of selected controls (section 1.6 and [3], Annex A).

(38) In addition, C-ITS station operators shall generate and maintain the following records as evidence of results achieved:

- records of training, skills, experience and qualifications ([3], clause 7.2);
- monitoring and measurement results ([3], clause 9.1);
- internal audit programme ([3], clause 9.2);
- results of internal audits ([3], clause 9.2);
- results of the management review ([3], clause 9.3);
- results of corrective action ([3], clause 10.1).

2. REFERENCES

The following references are used in this Annex:

[1] Annex III to this Regulation

[2] ISO/IEC 27000 (2016): Information technology – security techniques – information security management systems – overview and vocabulary

[3] ISO/IEC 27001 (2015): Information technology — security techniques – information security management systems – requirements

[4] ISO/IEC 27005 (2011): Information technology – security techniques – information security risk management

[5] ETSI TR 102 893 V1.2.1, Intelligent transport systems (ITS) – security; threat, vulnerability and risk analysis (TVRA)

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[7] ETSI EN 302 637-2 V1.4.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 2: Specification of cooperative awareness basic service

[8] ETSI EN 302 637-3 V1.3.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 3: Specifications of decentralised environmental notification basic service

[9] ETSI TS 103 301 V1.2.1: Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Facilities layer protocols and

communication requirements for infrastructure services

[10] A European strategy on cooperative intelligent transport systems – a milestone towards cooperative, connected and automated mobility (COM(2016) 766, 30 November 2016)

[11] ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[12] ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing

[13] ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS); Communications architecture

[14] ETSI TS 103 097 V1.3.1. Intelligent transport systems (ITS) security; security header and certificate formats