Annex A.1

A.1 justification for proposed draft new Recommendation

Question:	4/17	**Proposed new ITU-T Recommendation**	Geneva, 22 – 30 March 2017	
Reference and title:	ITU-T X.ucstix "Use Cases for Structured Threat Information Expression (STIX™) "			
Base text:	COM17-C.0076 Annex A.2		**Timing:**	2019-09
Editor(s):	Jong-Hyun Kim, ETRI, Korea (Republic of), jhk@etri.re.kr Ik-Kyun Kim, ETRI, Korea (Republic of), ikkim21@etri.re.kr		**Approval process:**	TAP

Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability):

This Recommendation aims to provide various use cases for Structured Threat Information Expression (STIX™) which is a structured language for describing cyber threat information. It is targeted to support a range of core use cases involved in cyber threat management, including analyzing cyber threats, managing response activities, sharing cyber threat information and etc. These use cases are typically simple in nature and do not convey the full expressivity or flexibility of the STIX language. The use cases include some implementations, XML representations of STIX content, and fully validated STIX content documents. The STIX suite of specifications is the responsibility of OASIS. See <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti>

Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work):

For real-time response to cyber threats, not only individual security systems, but also global cooperative security management systems should be provided since there are global problems which cannot be solved by any single entity as well as single domain. Therefore, global cyber threat intelligence is an important component of an organization's security program and can be obtained internally and from external sources. One of solutions for cyber threat intelligence and information sharing is Structured Threat Information Expression (STIX™) which is a structured language for describing cyber threat information. STIX provides structured representations of cyber threat information that is expressive, flexible, extensible, automatable, and readable. The STIX suite of specifications is the responsibility of OASIS. See <https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti>

The purpose of this draft Recommendation is to provide various use cases for how the STIX language may be used to support the cyber threat intelligence and information sharing context. This draft Recommendation also describes concepts and functionality of Structured Threat Information Expression (STIX™). It is targeted to support a range of core use cases involved in cyber threat management, including analyzing cyber threats, managing response activities, sharing cyber threat information and etc. Given this kind of information, a security decision can be made on how to best defend against the threat. It is intended to support both more effective analysis and the continued exchange of cyber threat information.

Relations to ITU-T Recommendations or to other standards (approved or under development):

ITU-T X.1500, ITU-T X.1500 Amendment 10

Liaisons with other study groups or with other standards bodies:

OASIS, ETSI

Supporting members that are committing to contributing actively to the work item:

Korea (Republic of), ETRI, KISA,