**3GPP TSG-SA3 Meeting #107Adhoc-e *S3-221451***

**e-meeting, 27th June – 1st July 2022**

**Source: Intel**

**Title: Anomaly in Multivendor NWDAF Framework**

**Document for: Approval**

**Agenda Item: 5.8**

# 1 Decision/action requested

***This pCR adds a key issue to TR 33.738.***

# 2 References

[1] 3GPP TR 23.700-81: " Study of Enablers for Network Automation for 5G System (5GS); Phase 3"', Rel.18.

# 3 Rationale

In 3GPP NWDAF-based architecture [6], the Multivendor sharing of MTLF or ML Models are being discussed in Rel-18. This sharing provides opportunities and challenges. The opportunity is the ability to efficiently share the ML models with consumers with lower complexity and dynamically. However, the challenges are that AI/ML model components, trained from data, are black boxes. When inputs are presented (whose goal is to discover something about the model vulnerabilities), it is unlikely for the target to detect that it is being gamed into revealing something during such a Multivendor sharing scenario. Therefore, this pCR proposes a key issue that describes the need for the ML model's anomalous behaviour to capture in the TR 33.738 related to the approved SID [1].

# 4 Detailed proposal

SA3 is kindly requested to agree on the pCR below to TR 33.738

\*\*\*\*\*Start of Changes\*\*\*\*\*

## 5.X Key Issue #X: Anomaly in Multivendor NWDAF Framework

### 5.X.1 Key issue details

In 3GPP NWDAF-based architecture [6], the Multivendor sharing of MTLF or ML Models are being discussed in Rel-18. This sharing provides opportunities and challenges. The opportunity is the ability to efficiently share the ML models with consumers with lower complexity and dynamically. However, the challenges are that AI/ML model components, trained from data, are black boxes. When inputs are presented (whose goal is to discover something about the model vulnerabilities), it is unlikely for the target to detect that it is being gamed into revealing something during such a Multivendor sharing scenario.

Furthermore, the threat model for such multivendor sharing includes not-trust by definition. e.g., Vendor A may not trust B or C, and vice-versa, A, B, and C, all trust Operator contractually. They expect the Operator to be a responsible integrator that protects each vendor from the other.

Given the complexity of such an environment in an operator domain, ML models in MTLF need to:

a) Predict the anomaly in ML Models

b) Detect anomalies in ML models

c) Categorize the anomaly in ML models

d) Act to address the Anomaly in ML models.

### 5.X.2 Security threats

ML models in multivendor NWDAF architecture are black boxes and pose threats such as zero-day attack, improperly trained models, which can reveal the ML models between vendors.

### 5.X.3 Potential security requirements

5GS system shall detect anomalous ML models in the multivendor ML sharing scenarios.

Procedures on how to detect anomaly in ML Models is out of scope of the 3GPP and will be left to implementation.

\*\*\*\*\*End of Changes\*\*\*\*\*