**3GPP TSG-SA3 Meeting #115, AthensS3-24*xxxx***

**26 Feb – 01 Mar 2024**

**Source: Johns Hopkins University APL, US National Security Agency**

**Title:** **Updates to skeleton TR 33.757**

**Document for: Approval**

**Agenda Item: 5.3**

# Decision/action requested

***This pCR is proposing to add the Overview clause of TR 33.757***

# 2 References

# 3 Rationale

The contribution proposes content for the Overview clause of TR 33.757.

# 4. Detailed proposal

It is suggested to approve the following change.

\*\*\*\* START OF CHANGE \*\*\*\*

# 4 Overview

A NPN customer may deploy on-premises NFs, or hosted NFs which reside in thrid-party premises, or both. The term ‘NPN customer domain’ is used to cover these cases.

A PLMN hosting an NPN is an example of a Public Network Integrated NPN (PNI-NPN). The term ‘PNI-NPN’ applies to this study of a PLMN hosting an NPN.

Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN. [1] Therefore, NFs which may reside within PNI-NPN Network Slice instances may require interfaces which cross the operational domains between PNI-NPNs and PLMNs. In addtion, AFs which reside within a PNI-NPN DNNs operational domain may require interfaces which cross the operational domains between PNI-NPNs and PLMNs.

The creation, modification, and termination of a Network Slice Instance (NSI) are supported by Management Services provided by the 5G management systems. [2] Therefore, NFs which provide NSI Management Services may cross the operational domains between PNI-NPNs and PLMNs.

NFs which reside in the PNI-NPN operational domain may require interfaces which cross the trust boundary between PNI-NPN and PLMN. Therefore, these interfaces require security controls to mutually protect the NFs which reside in the PLMN operational domain and in the PNI-NPN operational domain.

\*\*\*\* END OF CHANGE \*\*\*\*