**3GPP TSG-SA3 Meeting #113 *S3-23xxxx***

**Chicago, USA 06 - 10 November 2023** (revision of S3-yyxxxx)

**Source: Huawei, HiSilicon**

**Title: Discussions on R19 SID for UAS security enhancement**

**Document for: Discussion**

**Agenda Item: 6**

# 1 Decision/action requested

***Provide more information to have a new study on network slicing.***

# 2 References

[1] 3GPP TR 22.843 Study on Uncrewed Aerial Vehicle (UAV) Phase 3

# 3 Rationale

3GPP SA1 is completing its UAS phase 3 study with new requirements to further enhance safety and security of drone operations [1]. The following potential security issue should be studied in SA3 to ensure the safety and security of UAV operations.

## 3.1 Potential DoS or Depletion-of-Battery (DoB) attacks to UAV

An UAV is defined in 3GPP as a 2-in-1 device, i.e. an UAV can be seen as a UE with normal SIM as well and it may have two different services at the same time: UAV services and non-UAV services. The QoS of UAV services may not be met if other non-UAV services occupy too much network resources. Also, it seems to be possible that an attacker UE can initiate non-UAV services maliciously. For example, an attacker can initiate a new PDU sessions with a UAV and send large amount of data (video/unrelated files etc) to exhaust UAV’s network resources or deplete its battery. It may cause hazardous situation or safety concerns if not handeled properly.



**Observation 1:** Its worthwhile to investigate whether such a DoS attack or DoB attack is feasible, i.e. whether it may cause safety/security issues to the operations of UAVs or degrade the QoS/QoE of UAV services, especially when the UAV is in mission.

# 4 Detailed proposal

It is proposed to study DoS/DoB attacks and potential security enhancements to UAS in R19.