安全能力：

1、IPS/IDS、抗DDoS设备、防病毒软件、安全配置核查、主机配置防篡改等安全机制截图

2、物联网卡管控平台的截图

UPF：

1. 5G 专网应开启NAS层机密和完整性保护，能够对NAS信令进行机密性和完整性保护。（如果企业不具备或未开启加密机制，需要提供说明材料。）

核心网侧确认是否在AMF上开启NAS加密

1. 5G专网N4接口是否支持物理隔离，或者具备机密性保护、完整性保护和抗重放保护机制。

提供UPF侧LST IPSECPROPOSAL、LST IKECFG的查询截图

1. N4接口应支持双向认证能力或仅允许指定IP的SMF和UPF互访。如使用NRF进行注册和授权，则未在NRF中合法注册和授权的SMF无法访问UPF。

确认是否通过NRF进行SMF和UPF的对接；若采取IP配置互通，则于UPF侧提供LST CPNODEID和LST CPACCESSLISTFUNC、LST CPACCESSLIST的截图。

说明是否存在双向认证机制。

1. 边缘UPF应支持启停/链路中断告警，当UPF重启/断电/链路中断后，维护终端/网管上均能生成告警记录。

提供UPF告警日志记录截图

1. UPF应支持信令面/用户面流量控制机制，以确保其在收到大量攻击报文时不会产生异常。

提供UPF LST LBFC， LST DDOS的查询结果截图

1. 边缘UPF应支持IPSec加密、访问控制等安全功能。

提供UPF 的LST ACL、LST SECPOLICY、DSP ACLRULEADV4的查询结果截图

1. UPF应支持分流策略安全机制，可进行分流策略的配置、冲突检测和告警。

提供UPF的LST COLOCATEDLBO， DSP COLLISIONCHECK，LST QOSAPPLICATION的查询结果截图。对于有多个参数可选的，提供所有可选参数的查询结果。

1. UPF应支持对UE的互访限制和访问控制，支持UE之间互访策略设置、DNN ACL策略配置，支持禁止园区私网主动访问运营商网络。

提供UPF的LST APNUEMUTACC和LST GLOBUEMUTACC、，LST ACLRULEADV4，LST ACLBINDAPN的查询结果截图。

1. 应从计算、存储和网络资源等方面加强网络虚拟化基础设施安全保障，对网络虚拟设施的所有操作应纳入统一管理平台，实现集中访问控制和安全审计。

提供登录网元时4A接入界面截图，并说明4A的访问控制和安全审计功能。

1. 应根据不同虚拟机功能合理划分内部安全域，做好域间隔离和访问控制。

提供UPF底层Fusionsphere的VPC/VDC等逻辑隔离和访问控制功能截图

1. 应支持切片网元隔离，确保非共享网元只出现在一个切片中。

提供UPF等下沉网元的LST SNSSAI、LST SLICEINSTINFO查询截图。

1. 查看虚拟机是否专用、物理机是否专用，以保障切片资源隔离。

提供UPF等下沉网元底层Fusionsphere的资源分配情况，说明虚机提供的功能以及物理机位置。

AMF/SMF：

1. 核查5G核心网AMF网元相关配置，确认已提供NAS层信令机密性和完整性保护的能力，登录AMF输入LST NGALGPRIORITY。
2. 核查专网网元服务化接口协议是否采3GPP标准要求的HTTP2.0协议及参数配置，且TLS保护功能正常开启. 输入MML命令：LST TLSCFG或LST INNERTLSMODE，核查相关配置。