5G行业应用安全风险评估初步资料需求

**（针对每一个问题，请逐项应答，逐一附证明材料）**

**文档部分：**

## 管理制度

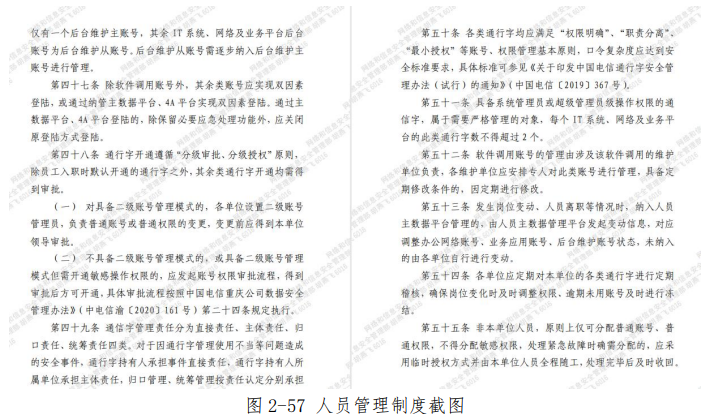
1. 说明是否建立5G行业应用安全风险评估管理办法、5G行业应用项目清单管理制度（内容应包括评估清单更新、应用定期核查、风险台账管理等风险管理机制）以及绩效考核及责任追究制度（应将5G行业应用安全管理纳入该制度）

提供上述制度文件及其对应要求内容的标注、截图等证明材料。如均由管理办法规定，则需分别提供对应条款。（信安部提供）



1. 说明是否针对关键岗位人员建立安全管理制度，并依据人员管理制度进行严格管理。

提供关键岗位人员安全管理制度文件（信安部提供）



1. 说明是否针对5G行业应用建立安全人员配置制度并配备相应的安全人员，且明确了各个角色的责任和权限。（信安部提供）

提供安全人员配置清单（信安部提供）、

内部人员发生变动（如换岗、离职）后的权限变更、删除记录或其他佐证材料（如审批记录和流程记录等）（网运、无优、客响、地市网运分别提供OMC账号申请、变更情况相关截图清晰版不用压缩-半年内的任意1-3张即可）



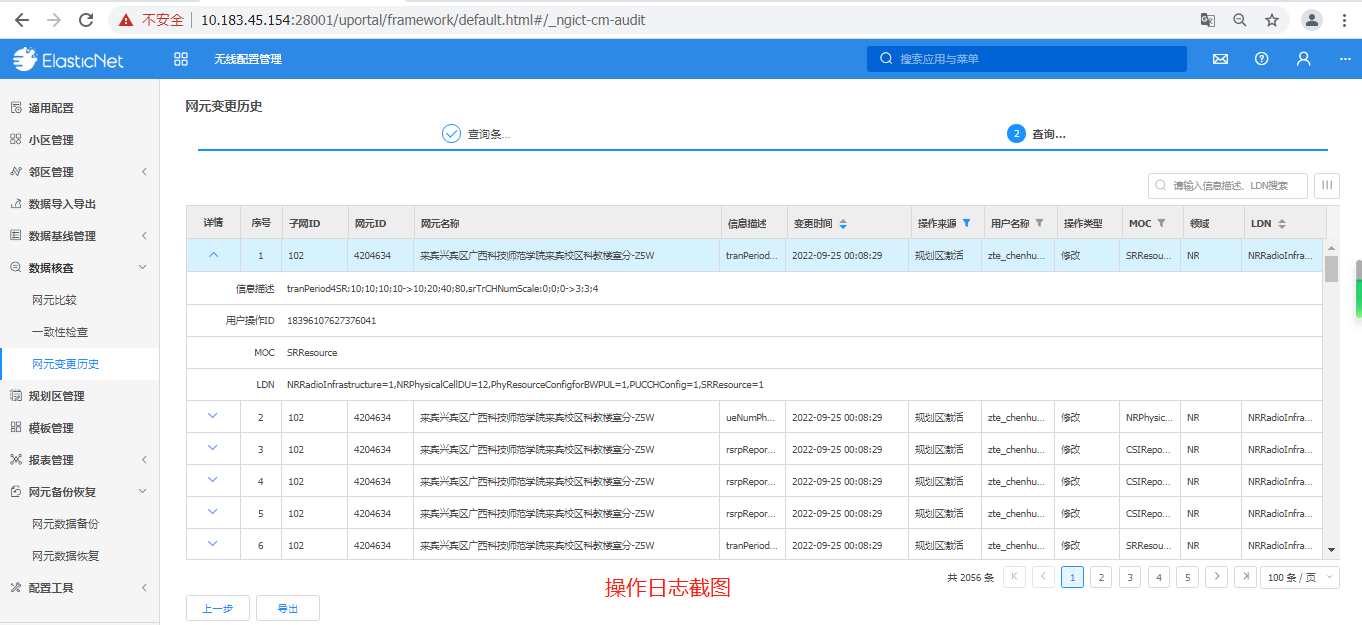
1. 说明是否针对5G行业应用建立安全运维管理制度并落实明确相应的安全运维人员、任务分工（信安部提供），

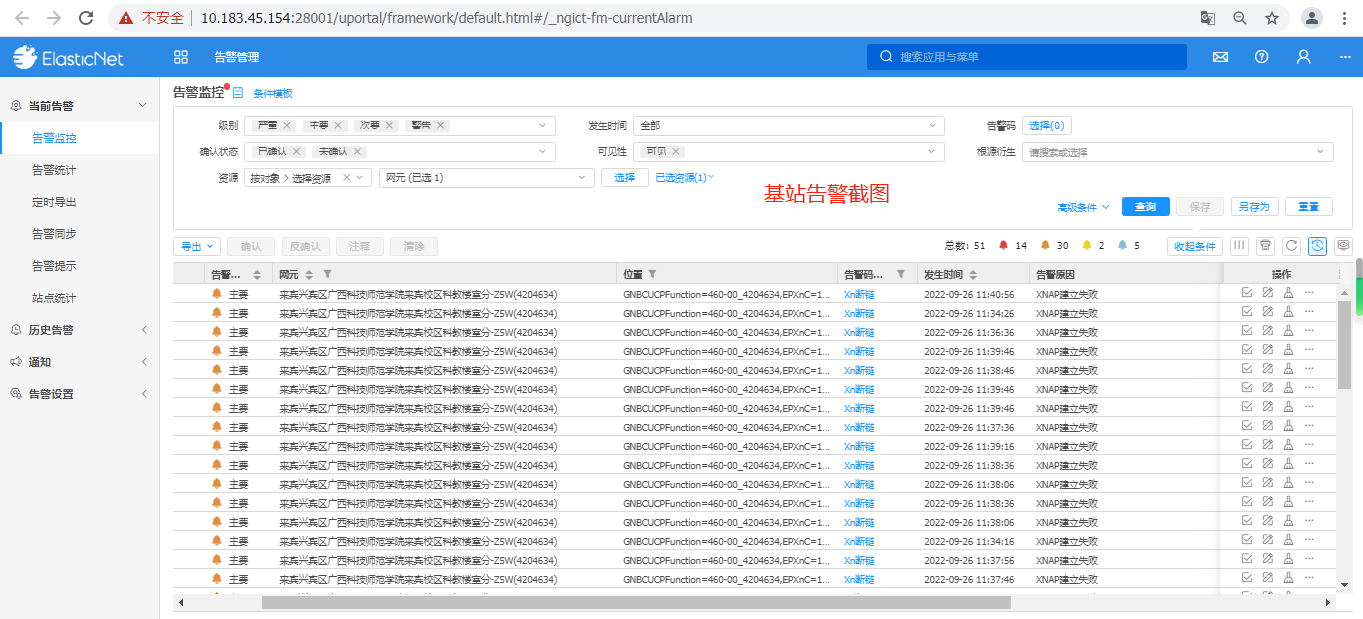
 

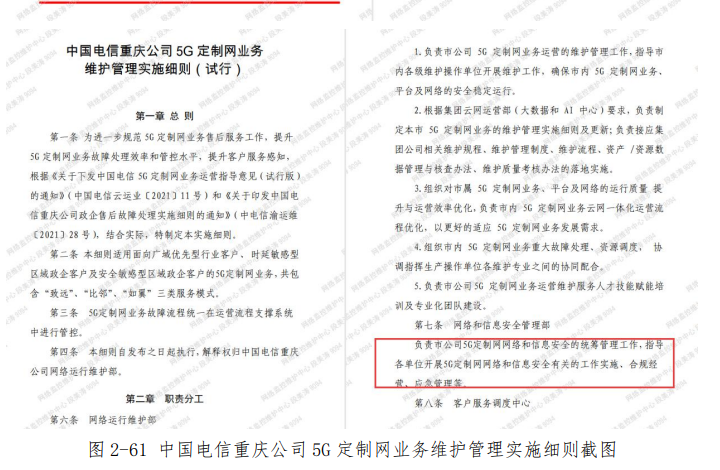
详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。（网运、无优、客响、地市网运分别提供OMC参数调整记录、OMC告警记录相关截图清晰版不用压缩-半年内的任意1-3张即可）













1. 说明是否记录和保存5G行业应用的相关基本配置信息及更新情况

提供5G行业专网网络拓扑结构（客响提供粗的）、各个专网设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等佐证材料（客响及地市网运提供）。

1. 说明是否建立针对5G行业应用相关的管理和运维系统，建立账号权限管理机制。

提供相关机制文档材料，内容应体现存在专门的部门或人员进行账号管理，对申请账号、建立账号、删除账号等进行控制。（网运中心提供）



1. 说明是否建立应急管理办法，并指定安全事件报告和处置管理制度。

提供相关办法和制度文件，并提供针对不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等明确条例。（信安部提供）

1. 说明是否指定不同事件的应急预案，并定期进行应急预案培训和演练。

提供相关文档的证明材料，应体现存在配套应急管理小组及相关资源保障，以及提供定期进行培训和演练的记录文档以及发现的弱点事件等记录文档。

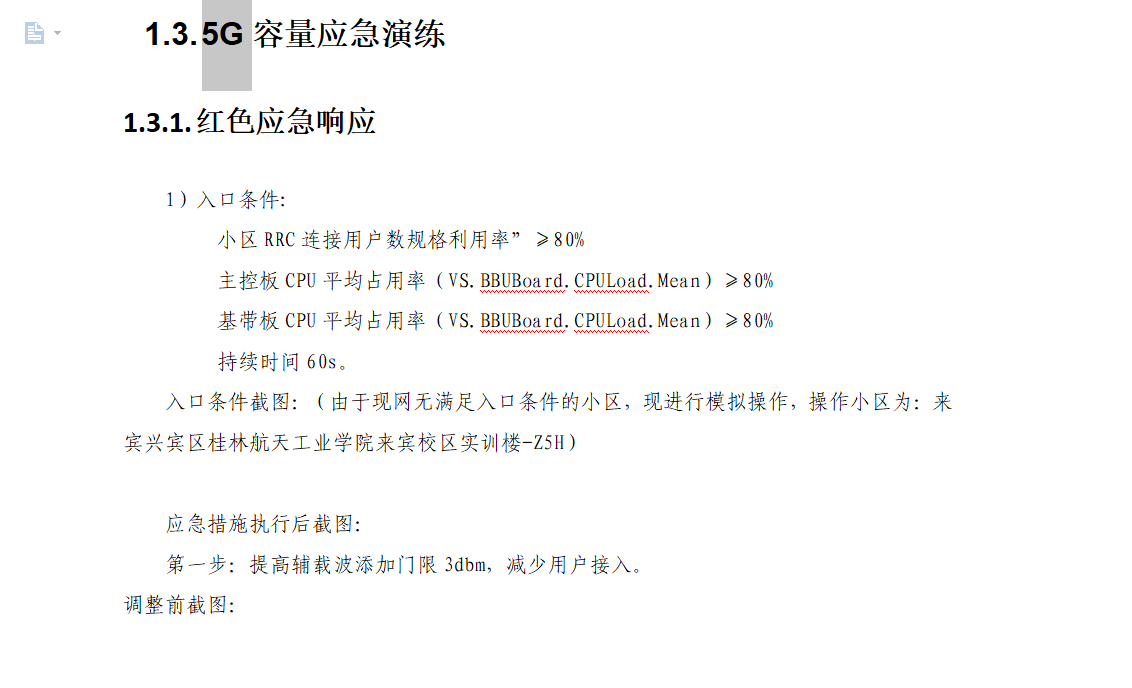
（信安部提供应急制度；

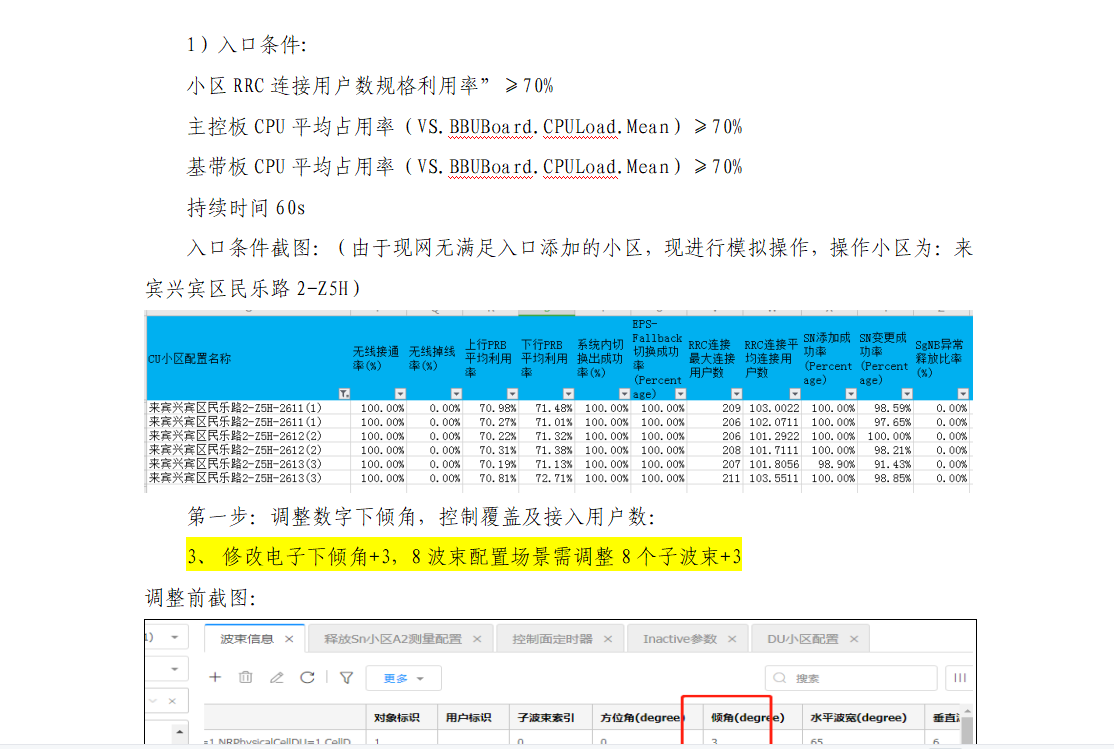
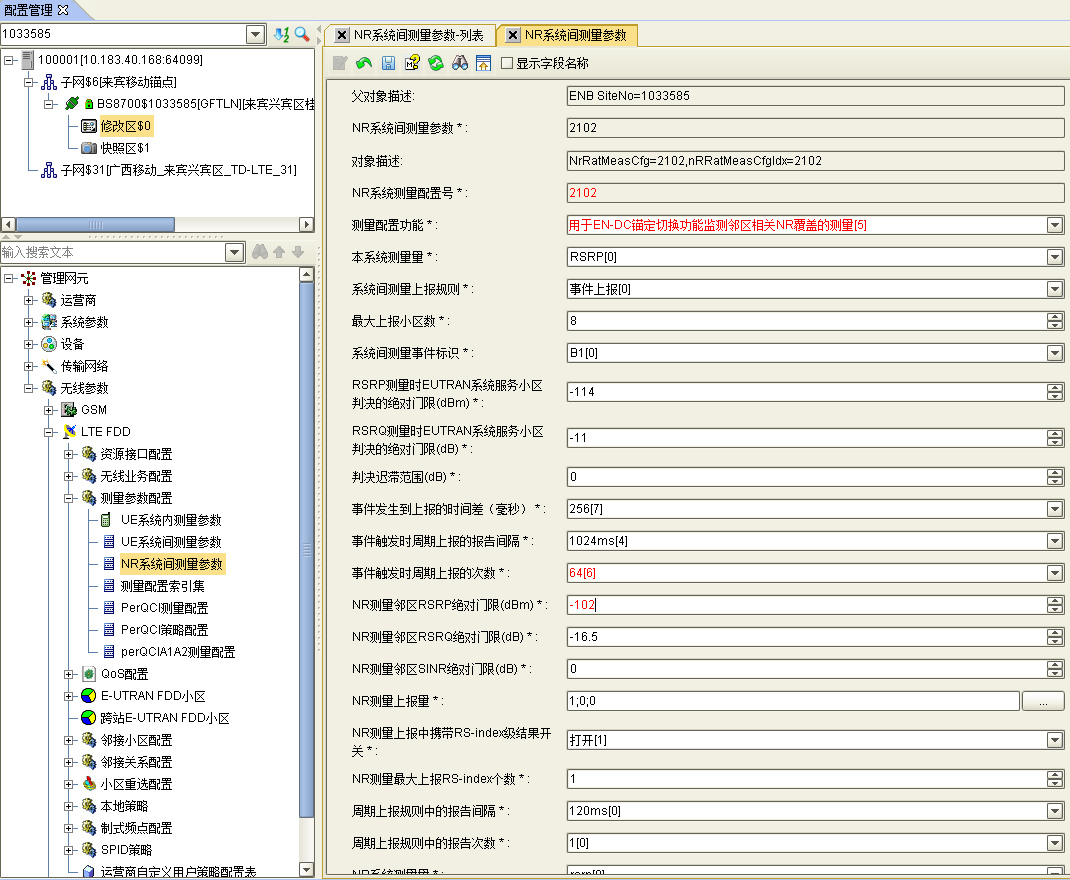
网运、无优、地市网运分别提供核心网侧、无线侧应急演练记录；

网运安全室提供安扫记录）









## 基本情况

1. 提供5G行业应用设计文档或其他说明材料，内容应至少包含5G行业应用名称，所属行业、业务场景、预计应用规模（开卡数量、5G终端数量、总终端数量等）、行业应用类型、设备部署位置及规划、第三方云服务使用情况、切片使用情况及类型、专网模式、行业应用简介、网络拓扑图、业务流量和特性、各项资产和运维责任归属情况等。（计划部、政企、客响分别提供设计方案文档）
2. 说明5G终端和接入网关应支持3GPP标准的认证机制，并支持3GPP标准中要求的机密性和完整性保护算法（如128-NEA1,128-NEA2,128-NEA3,128-NIA1,128-NIA2和128-NIA3）

提供5G终端和接入网关等的认证机制和加密算法的说明文档。（政企部）

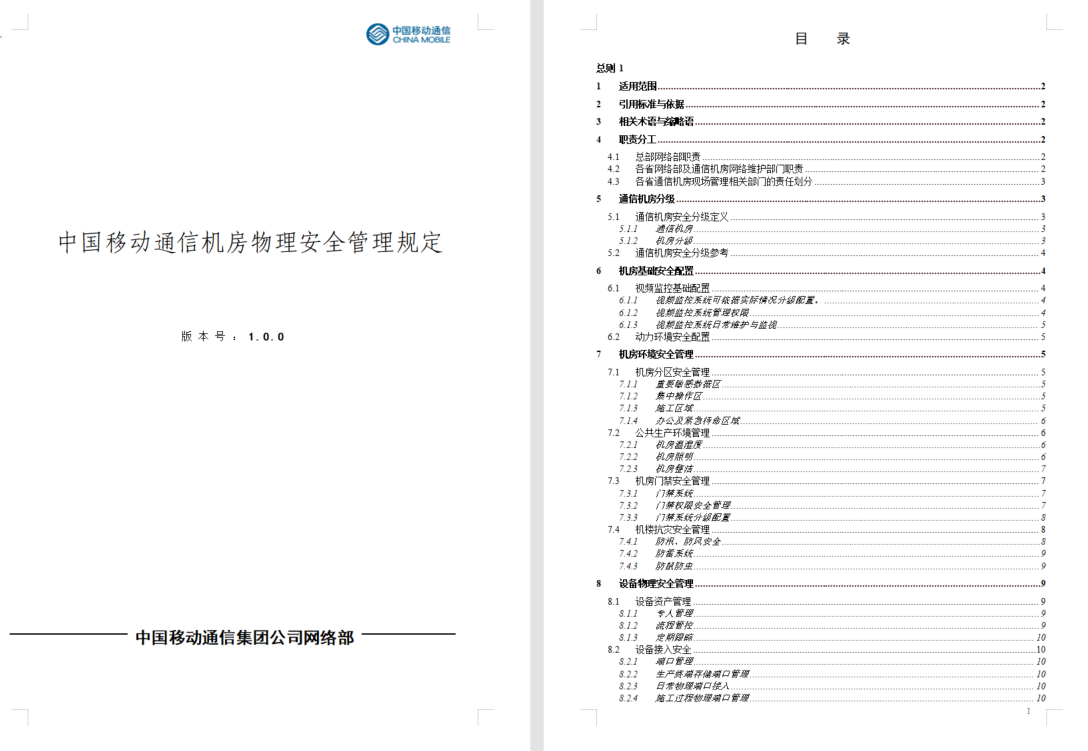
1. 说明该项目是否存在多方合作。若存在合作则应提供合作方式合规性评估记录文档和合作企业的安全保障能力评估记录文档。（政企部，可以参考以下附件中任何一个来做）



1. 说明该项目是否采用了第三方云服务。若存在第三方云服务，则应提供针对第三方云服务商的身份与资质证明材料；针对第三方云计算应提供安全保障技术和安全管理制度文档。（政企部）
2. 说明新建5G应用平台物理安全的安全保障措施，提供安全技术措施文档和安全管理制度文档，明确应用服务器、机房、节点的地理位置，应具备一定的管理措施和技术措施确保其物理环境安全。

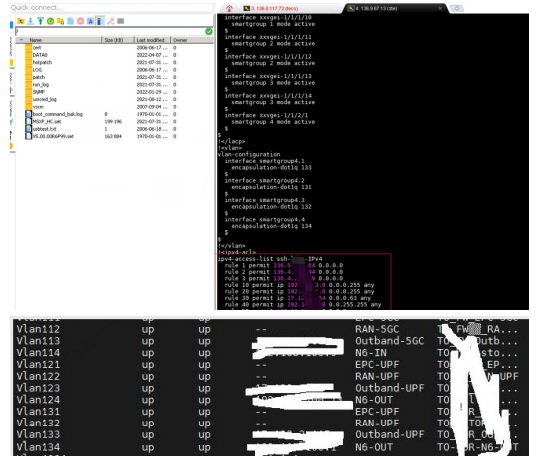
（信安部提供制度）





## 其他文档

1. 说明专网和公网之间的安全隔离和划分情况，提供拓扑图、防火墙安全策略配置和VPN配置（若存在防火墙）、DCGW上不同接口的VLAN划分情况等。（网运、地市网运提供）





1. 说明是否存在MEP。若存在MEP则应提供MEP的功能说明文档或界面，明确MEC APP对MEP API调用的认证和授权机制，以及对接入 MEP 的 MEC APP 进行安全认证、访问控制、操作审计和生命周期管理，对通信内容采用传输加密机制或协议等功能点。（计划部提供设计方案）
2. 说明是否存在切片配置。若存在端到端切片配置，则应提供切片管理域、切片运维域、切片与企业园区之间、切片与MEC之间设置隔离和访问控制措施的设计文档或配置文档；提供支持防终端NSSAI篡改攻击、防UE非授权跨切片访问攻击、防UE跨切片数据包重放攻击的说明配置文档。（计划部提供设计方案）
3. 若存在端到端切片配置，应说明切片隔离管理机制，提供相关文档材料；支持多种隔离手段，可按需做好端到端切片隔离和网络分段管理，使得某一网络故障或遭受攻击时不会影响其它网络的正常运行。（计划部提供设计方案）

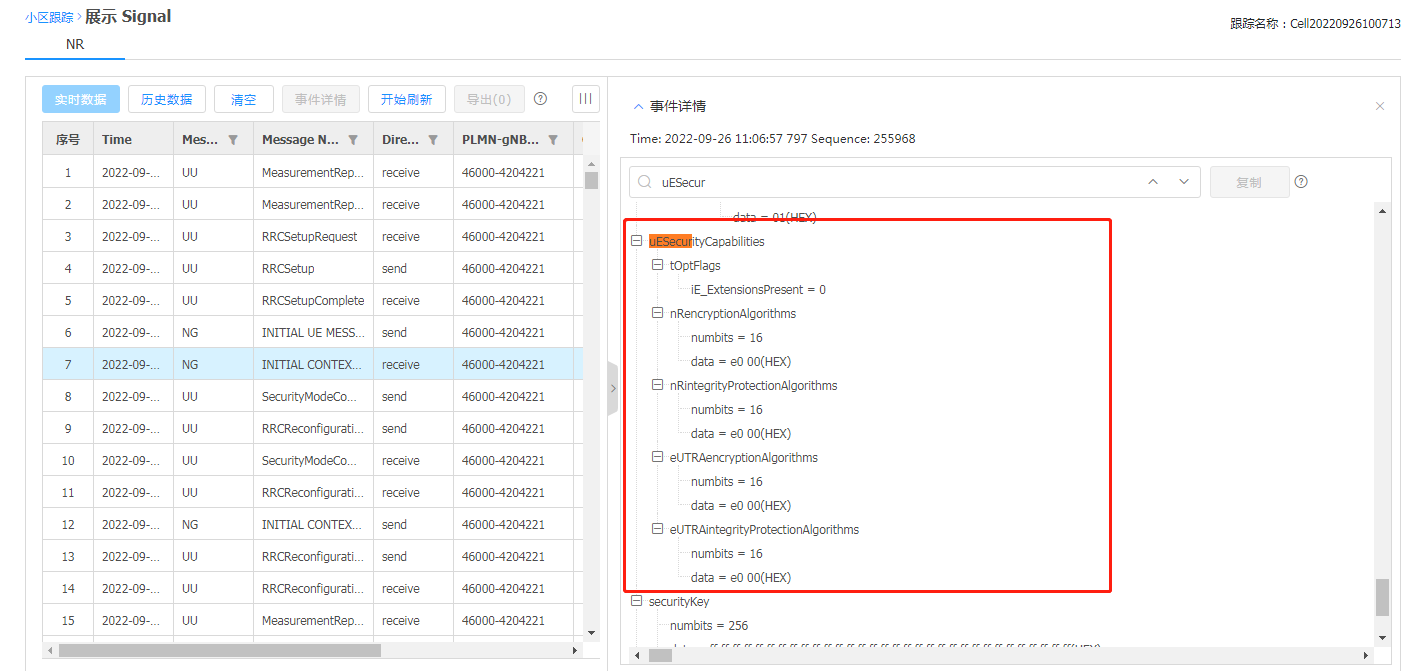
**操作部分：**

## 基站侧

1. 具备5G功能的终端和为行业终端提供接入服务的5G接入网关设备，应支持3GPP标准中要求的机密性和完整性保护算法，例如：128-NEA1,128-NEA2,128-NEA3,128-NIA1,128-NIA2和128-NIA3。

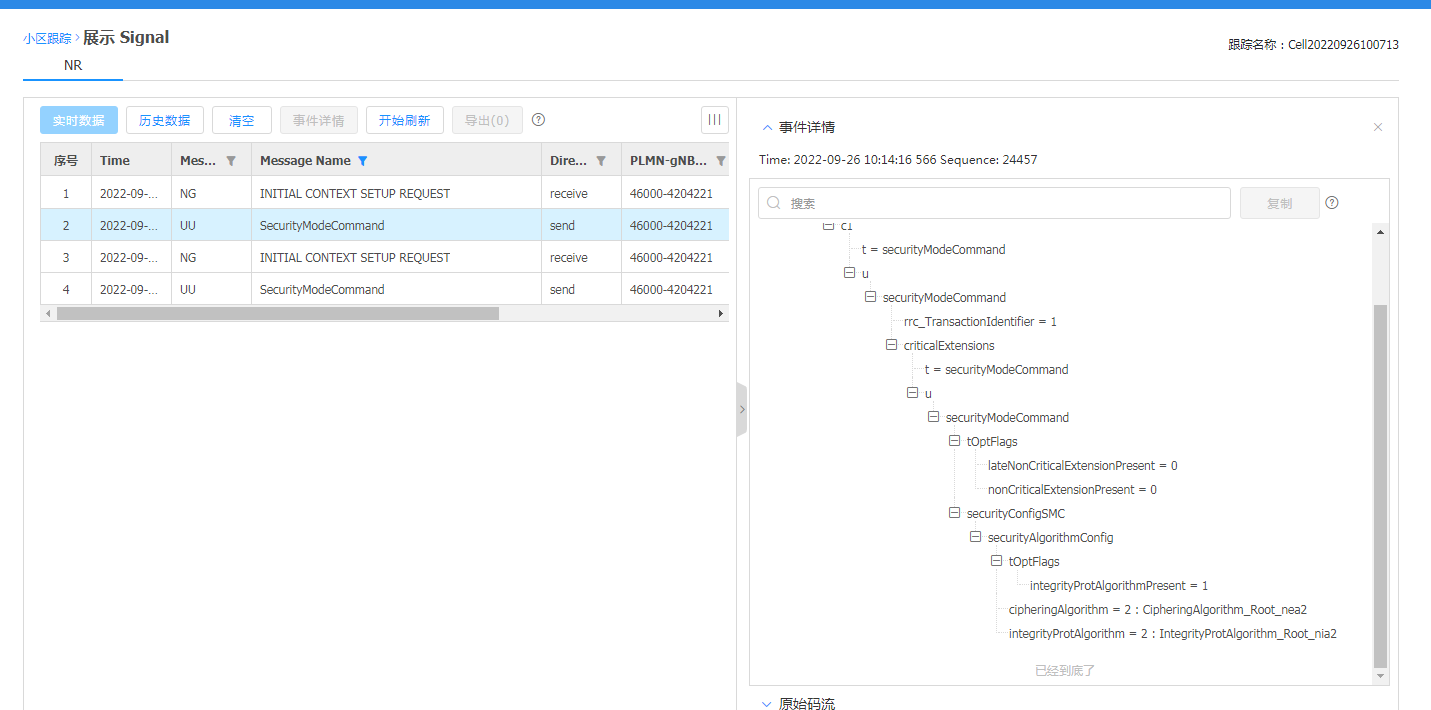
提供NG接口抓包中NGAP\_INIT\_CONTEXT\_SETUP\_REQ信令中uESecurityCapability字段截图





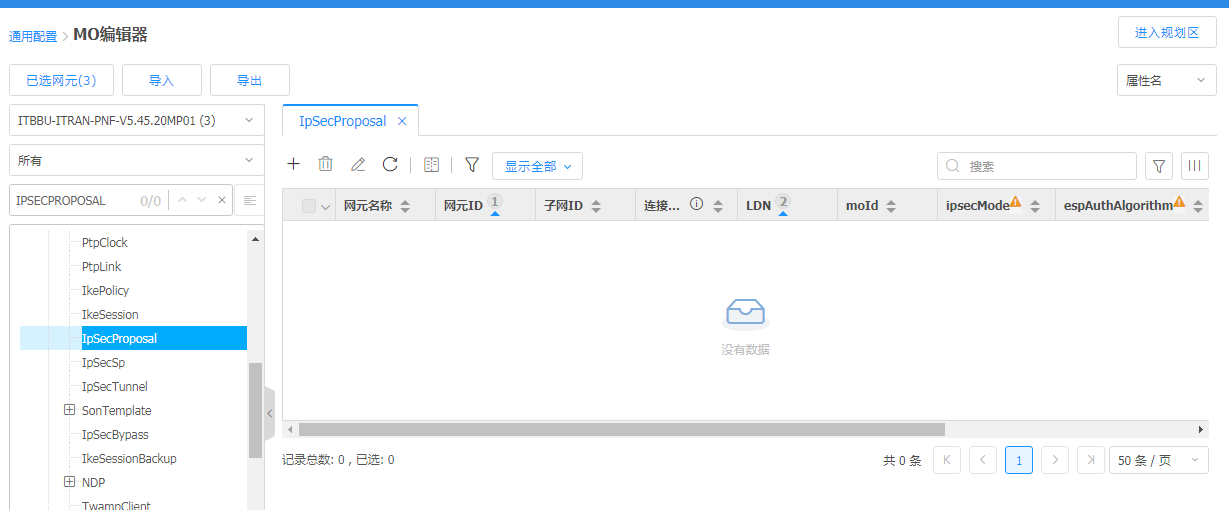
1. 5G专网gNB应开启AS层信令机密和完整性保护，能够对RRC信令进行机密性和完整性保护。(如果企业不具备或未开启加密机制，需要提供说明材料)

提供Uu接口抓包RRC\_SECUR\_MODE\_CMD报文securityAlgorithmConfig中cipheringAlgorithm和integrityProtAlgorithm字段值的截图



1. 说明5G专网N2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。

提供基站侧LST IPSECPROPOSAL、LST IKECFG的查询截图



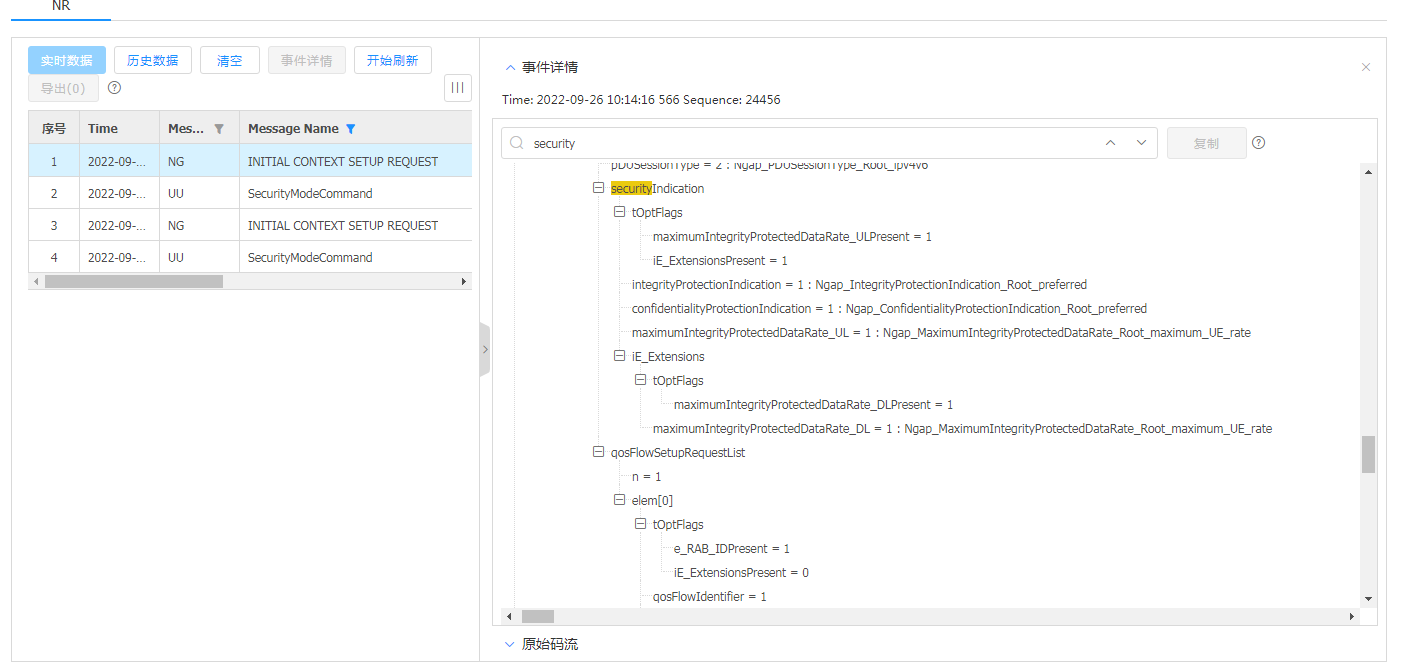
1. 5G专网gNB应支持机密性保护和完整性保护算法优先级配置，且完整性保护算法配置不能为NIA0。

提供基站LST GNBCIPHERCAPB和LST GNBINTEGRITYCAPB的查询截图



1. 5G专网应支持终端与gNB之间的用户面数据机密性保护机制，在有完整性保护/抗重放保护需求的业务场景下，5G专网应支持终端与gNB之间的用户面完整性保护/抗重放保护机制。

提供NG接口抓包NGAP\_INIT\_CONTEXT\_SETUP\_REQ报文的securityIndication字段，confidentialityProtectionIndication和integrityProtectionIndication值的截图



## 核心网侧

1. 5G基站或核心网支持对5G终端进行访问控制，仅允许特定的行业终端进入5G专网，限定条件包括但不限于终端标识（IMSI/SUPI）、终端位置（CGI、TAI）、IMEI黑名单、流量限制、机卡绑定等。

确认核心网侧是否针对该项目终端的接入做了额外配置；说明该项目网络中是否部署二次认证等安全能力，并提供证明材料。

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。

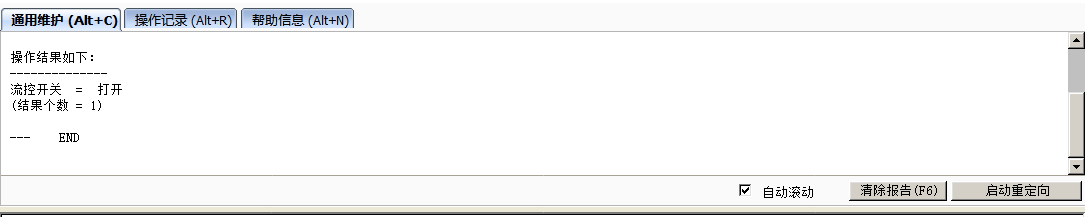
说明是否存在双向认证机制。

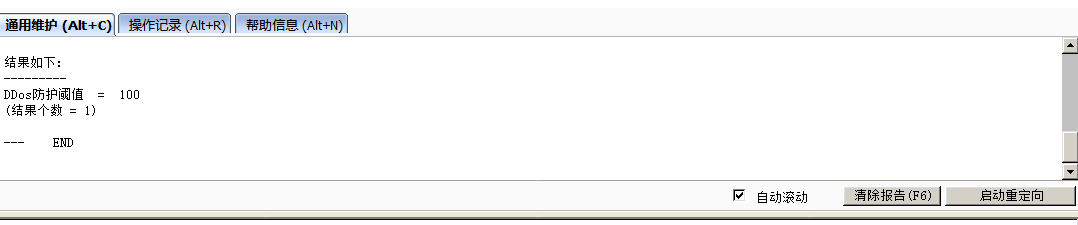
1. 边缘UPF应支持启停/链路中断告警，当UPF重启/断电/链路中断后，维护终端/网管上均能生成告警记录。

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. 应定期对物理/虚机操作系统、虚拟化软件、第三方开源软件实施安全加固。

提供系统物理/虚机操作系统、虚拟化软件、第三方开源软件定期安装补丁或更安全的版本等的截图，或相关台账记录等。

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。

## 数通设备

1. 5G专网应支持最小边界访问策略配置，仅允许必要的外部行业网络进行访问，默认禁止所有通信，不存在无效和多余的控制规则。

登录防火墙查看访问策略配置并提供完整截图，说明是否默认禁止，以及每条策略的功能和必要性。

1. 说明是否针对边缘UPF或下沉核心网，应根据行业应用需求部署防火墙、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。
2. 说明5G专网与公网之间是否根据组网情况进行物理或逻辑安全隔离。

登录DCGW和防火墙查看组网配置，提供VLAN和VPN划分截图，说明是否利用划分不同VLAN后VPN，对专网和公网进行隔离。

1. 若存在端到端切片配置，应说明切片隔离管理机制，提供相关文档材料；支持多种隔离手段，可按需做好端到端切片隔离和网络分段管理，使得某一网络故障或遭受攻击时不会影响其它网络的正常运行。

## MEC/MEP

1. 若存在MEC，则MEC部分应支持安全域划分，行业客户App应与运营商App、MEP、UPF处于不同的安全域，安全域之间应进行安全隔离。行业客户的应用之间、运营商自有应用之间也应进行安全隔离。

登录MEC数通设备或安全隔离设备，提供安全域配置、VLAN划分等能说明APP、UPF处于不同安全域的配置截图

1. 应具备边界访问控制安全能力，边缘云支持部署安全访问控制措施，可防止攻击者的非法访问。

提供MEC平台安全组、安全策略配置等功能点截图。

1. 应支持MEP启停告警，当MEP重启/断电后，维护终端/网管上均能生成告警记录。

提供MEP平台的告警日志记录。

1. 应支持MEP API调用安全，MEC APP对MEP的API调用需经过认证和授权。

提供MEP的API调用记录或认证授权记录，或相关功能配置点等的截图。

1. 应支持 MEP 与 MEC APP 的通信安全，对接入 MEP 的 MEC APP 进行安全认证、访问控制、操作审计和生命周期管理，对通信内容采用传输加密机制或协议。

提供MEP中安全认证、访问控制、操作审计、生命周期管理以及加密等功能点的截图。

1. 应支持MEP中虚拟机运行情况检测，可及时发现安全威胁。