投标人须知

**一、项目基本情况**

（一）项目名称：九龙现代产业集团2025年网络安全运维服务

（二）招标人：重庆九龙现代数字科技有限公司。

（三）项目概况：九龙现代产业集团需要对龙客在线系统、集团网络门户、集团电子大屏（两块）进行日常安全维护。一是在网络安全服务工作中以网络资产梳理及规划服务、安全基线核查服务、网络风险评估服务、网络安全巡检服务、扫描渗透服务、安全加固服务、应急演练服务、网络安全监测服务、应急响应服务、下属集团合规检查、信息与网络安全管理平台运维服务为抓手，实现集团网络安全“人防”技术支撑。二是健全完善集团的网络安全基础设施，部署国产化防火墙设备、终端安全监管平台、内容及播控安全防护平台的“技防”措施，构建覆盖"监测-防护-响应"的全方位安全防护体系。

**二、项目投标范围**

（一）服务内容：九龙现代产业集团2025年网络安全运维服务清单（附件4）。

（二）工期：自合同签署之日起一年。投标文件须满足谈判公告对工期的要求，否则其资格性、符合性审查不合格。

**三、投标人资格要求**

（一）具备有效的营业执照（须提供有效的营业执照副本复印件）；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障金的良好记录；

（五）参加采购活动前三年内，在经营活动中没有重大违法记录；

（六）本次招标不接受联合体投标，中选后不允许分包、转包。

（七）投标人具备信息系统安全运维服务资质认证（三级）。

**四、投标报价**

（一）本项目投标报价最高限价为295000元。投标总报价以元为单位，保留两位小数，小数点后第三位四舍五入，不足两位的按实际位数保留。

（二）投标人投标报价不得超过招标人公布的最高限价，否则按废标处理。

（三）本次报价须为人民币报价，报价包括本项目所有设计费、各种应纳的税费等完成本项目的一切费用。因投标人自身原因造成漏报、少报皆由其自行承担责任，招标人不再补偿。

五、付款方式

（一）合同签订后，中标人开具合同金额50%的发票，采购人在收到发票后15个工作日支付合同额50%的款项给中标方。项目验收后，中标方凭合同和验收报告提交合同金额50%的增值税普通发票，采购人在收到发票后15个工作日支付合同额50%的款项给中标方。

（二）本合同所约定价款均为含税价，中标方按现行税法规定及招标人要求开具增值税专用发票。

**六、投标文件要求**

（一）投标文件组成：

1、投标报价函（需加盖公司鲜章及法人签章）；

2、投标清单（需加盖公司鲜章）

3、有效公司营业执照复印件（需加盖公司鲜章）；

4、有效公司资质证书复印件（需加盖公司鲜章）；

5、授权委托书（加盖公司鲜章）；

6、承诺书（加盖公司鲜章）；

（二）投标文件制作

1、各投标人应当按要求编制投标文件，并对投标文件提出的要求和条件作出实质性响应，纸质文件原则上采用软面订本，同时应编制完整的页码、目录。响应文件**一式二份**（**两份响应文件应保持内容一致**，如投标人两份投标文件不一致，将按有利于招标人的一份投标文件进行评标）。

2、投标文件应采用档案袋密封，封皮上注明“项目名称”、“投标人名称”字样，档案袋的封口应加盖公章或法人授权代表签字。

七、投标文件的递交

（一）投标文件的递交时间：详见谈判公告。

（二）递交地点：重庆市九龙坡区二郎街道融堃•彩云里16楼。

（三）投标截止时间：详见谈判公告；

开标时间：同投标截止时间。

（四）**投标截止时间后送达的投标文件招标人不予受理；**

（五）谈判参与人员

**1.收到邀请书的投标人。未收到邀请的投标文件，招标人将拒绝接收。**

2.各投标人应当派1名代表参与，至少1人应为法定代表人或具有法定代表人授权委托书的授权代表。

**八、谈判程序及方法**

（一）谈判程序

1.投标人签到。

2.宣布谈判纪律，公布在投标截止时间前递交投标文件的投标人名称。

3.检查投标文件的密封情况。

4.随机开启投标文件，公布投标人名称、投标报价及其他内容，记录在表格上并由投标人确认签字。因投标人原因未签字确认，视为默认开标记录。

5.评标小组对所有投标人投标总价进行评审。总报价高于最高限价的，不进入报价排序；总报价低于最高限价的按报价**由低到高**的顺序进行排序。

6.评标小组按前述报价排序由低到高依次对投标人的资格条件进行资格性、符合性审查。

7.若排名第一的投标人资格性、符合性审查合格，则排名第一的投标人为中标人；若排名第一的投标人资格性、符合性审查不合格，且排名第二的投标人资格性、符合性审查合格，则排名第二的投标人为中标人，以此类推，直至选出合格中标人。

**注：**投标人应按谈判公告规定的时间和地点参加谈判并签到，否则其投标文件不得参与谈判。

（二）谈判方法

（1）评标小组的组建

由招标人按法律法规及相关规定依法组建评标小组。

（2）评标办法

**1.本项目采用经评审的最低价法。**

2.评标小组将资格性、符合性审查合格的投标人按报价（不高于最高限价）由低到高排序。

3.资格性、符合性审查合格的投标人中，报价最低的为中标人。若出现投标人投标报价一致的，由评标小组按照资质的高低原则排序；若出现投标人资质也一致的，由投标人进行第二次报价，直至报价区分出高低，报价最低的为中标人。

（3）评审标准

资格性、符合性审查内容：

1.资格性评审：投标人资格条件、信誉条件等。

2.符合性评审：投标文件格式、投标文件密封、盖章齐全、报价是否符合谈判文件要求等。

资格性、符合性审查中有任何一项不符合要求，其资格性、符合性审查不合格，不得成为中标人。

**九、中标人的确认**

（一）评审小组本着公开、公正、公平的原则，在按照比选标准比选结束后，比选结果在九龙现代产业集团网站（http://cqxpgyy.com/index/）上进行公示，公示期3天。

（二）若公示期间未收到异议或投诉，招标人将在公示期结束后3日内以书面形式向中标人发出中标通知书。

十、合同签订

招标人和中标人应当自中标通知书发出后按中标通知书要求，根据招标文件和中标人的投标文件订立书面合同。中标人无正当理不与招标人签订合同的，招标人取消其中标资格；给招标人造成的损失的，中标人应当赔偿。

十一、弃标处理

（一）在中标公示结束后三日内，中标人未按规定签订合同的，招标人将其列入重庆九龙现代数字科技有限公司信用黑名单，禁止在重庆九龙现代数字科技有限公司承揽相关业务。

（二）中标人放弃中标，给招标人造成损失的，应当赔偿，同时招标人将其列入重庆九龙现代数字科技有限公司信用黑名单，禁止在重庆九龙现代数字科技有限公司承揽相关业务。

（三）中标人放弃或者被取消中标资格时，招标人可按投标人须知第三部分第二条“谈判程序及方法”确定的原则依次序确定中标人，也可以重新组织谈判。

十二、重新招标

有下列情形之一的，招标人将重新招标：

1. 投标截止时间止，投标人少于3个的；

（二）经评标小组评审后否决所有投标的；

（三）法律法规规定的其他需重新招标的情形。

十三、其他

除前文要求外，投标人发生以下条款情况之一时，视为无效投标，其投标文件将被拒绝：

（一）投标人不符合规定的资格条件的；

（二）投标人的法定代表人或其授权代表人未签到参加谈判的；

（三）法定代表人为同一个人的两个及两个以上法人，母公司、全资子公司及其控股公司参与谈判的；

（四）单位负责人为同一人或者存在直接控股、管理关系的不同投标人；

（五）投标人投标文件内容有与国家现行法律法规相违背的内容，或附有招标人无法接受的条件的。

**附件1**

### （一）投标函

 （招标人名称）：

1．我方已仔细研究了 （项目名称）招标文件的全部内容，愿意以人民币 元（大写： ）的总价作为本次投标的总报价，质量技术要求及验收方法：满足竞争性谈判文件要求，工期 日历天。

2．我方承诺在投标有效期内不修改、撤销投标文件。

3．如我方中标：

我方承诺在收到中标通知书后，在中标通知书规定的期限内与你方签订合同。

4． （其他补充说明）。

投标人：　　　　　（盖单位章）

法定代表人或其委托代理人：（签字）

地址：

电话：

传真：

邮政编码：

年 月 日

注：大写金额和小写金额不一致时，以大写金额为准；

**附件2：**

法定代表人身份证明书

项目名称：

致：（招标人名称）：

（法定代表人姓名）在（投标人名称）任（职务名称）职务，是（投标人名称）的法定代表人。

特此证明。

（投标人公章）

年 月 日

（附：法定代表人身份证正反面复印件）

法定代表人授权委托书

项目名称：

致：（招标人名称）：

（投标人法定代表人名称）是（投标人名称）的法定代表人，特授权（被授权人姓名及身份证代码）代表我单位全权办理上述项目的谈判、签约等具体工作，并签署全部有关文件、协议及合同。

我单位对被授权人的签字负全部责任。

在撤消授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤消而失效。

被授权人： 投标人法定代表人：

（签字或盖章） （签字或盖章）

附被授权人身份证复印件

**附件3：**

**承诺书**

 （招标人名称）：

 我单位 （投标人全称）在充分理解 （项目名称）竞争性谈判文件要求的基础上，郑重作出如下承诺，并愿意承担相应的法律责任：

（一）具有良好的商业信誉和健全的财务会计制度；

（二）具有履行合同所必需的设备和专业技术能力；

（三）有依法缴纳税收和社会保障金的良好记录；

（四）参加采购活动前三年内，在经营活动中没有重大违法记录；

（五）本次投标不采用联合体投标，中选后不分包、转包。

 投标人：　　 　　　（盖单位章）

法定代表人或其委托代理人：（签字）

年 月 日

**附件4：**

**九龙现代产业集团2025年网络安全运维服务清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务分项** | **服务概述** | **数量** | **投标报价（元）** |
| 1 | 网络资产梳理及规划服务 | 1.通过对集团内部机房线路、设备、安全策略、资产信息进行台账整理管理（包括梳理互联网出口、专网出口、网络区域划分情况、网络-安全-服务器等设备接口连接情况、IP规划情况等），对现有的信息资产情况进行了解，更好的提供系统的运行维护服务。2.资产指纹梳理：对内网、互联网端口及服务进行测绘，如：端口、服务等。3.网络安全架构及规划设计包含顶层设计技术咨询与安全规划、专项技术路线设计，规划设计范围覆盖但不限于：网络安全专项设计、终端 接入安全专项设计、应用安全专项设计、数据安全专项设计、业务安全专项设计、身份安全专项设计、系统安全专项设计、密码安全专项设计、个人信息保护安全专项设计等专项技术领域设计。4.业务应用探测：不同WEB容器识别，如：Apache、tomcat、Weblogic、WebSphere和Nginx等；多种服务端语言探测，如：PHP、JSP、ASP、ASPX和.NET等；WEB前端框架探测，如：jQuery、Bootstrap、HTML5等；WEB后端开发框架探测，如：Django、Rails、ThinkPHP、Struts等； WEB业务应用探测，如：BBS、CMS和BLOG等。5.云上资产审计：根据上云状况对存在云端的重要系统、自查进行统计，梳理出云上资产信息以方便开展后续工作（此项在签署合同时应注明甲方、云厂商的配合工作，提供我单位云上资产的相关权限）。 服务频率：全年2次，每半年1次。输出材料：《资产管理清单》、《网络拓扑图》 | 1项 |  |
| 2 | 安全基线核查服务 | 1.依据业界主流基线标准，对招标人重要信息系统相关网络设备、安全设备的配置以及业务系统中应用程序的配置情况进行核查，判断是否符合安全性要求，是否存在安全风险和隐患，并能根据不同业务系统的要求，提供相应等级的设置建议。2.基线核查范围：服务器、应用系统、数据库、中间件、网络设备、安全设备。服务频率：全年2次，每半年一次。交付材料：《基线核查报告》 | 1项 |  |
| 3 | 网络风险评估服务 | 依据相关规范，在业主方允许的情况下，对目标范围内的系统资产、威胁、脆弱性等各方面进行评估，对主要资产的风险进行定性或定量的脆弱性风险分析，描述不同资产的风险高低状况，给出详细的风险评估报告、整改方案及技术支撑。服务频率：全年4次，每季度1次。交付材料：《网络风险评估报告》 | 1项 |  |
| 4 | 网络安全巡检服务 | 1.对重要的信息系统服务器、核心网络设备及安全设备进行设备健康状态检查、策略配置维护等服务；2.根据安全策略检查与维护情况，提交检查与维护记录；3.安全巡检服务范围包括安全设备、服务器安全状况等；4.巡检工作结束后，围绕本次的巡检工作，总结此次发现的问题，针对问题提出相应的处置方法与建议；服务频率：全年4次，每季度1次。输出材料：《季度、日常巡检报告》 | 1年 |  |
| 5 | 扫描渗透服务 | 依据相关规范，通过远程或者现场方式使用专业的漏洞扫描工具对信息系统进行全面漏洞扫描工作，为安全加固提供安全建议。漏洞扫描工具需满足以下要求：（1）具备资产探测梳理、主机漏洞扫描、网站漏洞扫描、基线配置核查等，支持二级域名扫描功能，输入一级域名进行一键扫描，通过搜索互联网数据，自动获取到该域名的二级域名、网站标题、解析IP地址（提供工具界面截图证明）；（2）支持IP反查域名监测，输入IP或者网段，通过搜索互联网数据，自动获取到IP对应的域名、url链接、网站标题、返回状态码（提供工具界面截图证明）；（3）支持漏洞利用证明，通过POC验证过的漏洞，扫描结果需包含漏洞利用证明，包括但不限于攻击Payload、目标响应结果、漏洞利用点、关键参数等内容（提供工具界面截图证明）；（4）支持渗透测试台账，支持以excel报表格式导入渗透测试报告，形成渗透测试台账。可在系统查看渗透测试结果，以图表形式可视化展现漏洞风险级别比例、风险应用比例，可对渗透报告中的漏洞进行跟踪确认，处置漏洞状态：未整改、已整改、忽略、未整改（提供工具界面截图证明）服务频率：全年4次，每季度1次。交付材料：《漏洞扫描渗透报告》 | 1年 |  |
| 6 | 安全加固服务 | 针对安全服务过程中发现的各类安全问题，按照风险等级进行划分，给出解决方案，及时协调对应供应商进行加固整改和安全优化。对于不能修复的漏洞，提供详细情况说明。1、加固范围：基于风险评估、渗透测试、漏洞扫描、基线核查、安全巡检结果进行针对性整改。2、对于设备老旧、影响业务连续性、特殊原因等导致的无法直接进行加固的情况可通过在安全设备上增加策略，封禁端口，增加其他自定义规则的方法完成加固。3、对服务过程中已发现的问题提出加固建议，整改方案，方法，意见，技术措施等并协助供应链厂商进行加固。4、对于无供应链厂商的情况可主动提供加固服务，加固内容包含安全设备、主机、应用系统、数据库、中间件等。5、对未能实施加固（残余风险）的风险项进行详细说明，并提出安全补救措施和安全专家建议，为管理人员的后期维护提供参考。6、本项为专业安全服务，涉及面广，技术要求高，需配备项目负责人一名，同时具有CCIE网络、RHCE系统、OCP数据库、IBM存储专家等国际主流技术资质（需同时提供人员资质证书复印件并加盖投标人公章）。服务频率：全年4次，每季度1次。交付材料：《安全加固报告》 | 1年 |  |
| 7 | 应急演练服务 | 为全面做好2025年-2026年集团网络安全保障工作，确保重要信息系统和网络的安全稳定运行，切实落实单位突发事件的防范和应急处理工作，提高单位预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，依据《国家网络与信息安全事件应急预案》，并结合我区信息系统现状，制订演练方案。包括提供服务器，攻击测试环境搭建，脚本编写，剧本编写，明确演练目标以及参加演练的系统；演练前做好各项准备工作，并对参加演练的相关人员进行必要的培训，保证演练达到预期目的。服务频率：一年一次。输出材料：《应急演练脚本》 | 1项 |  |
| 8 | 网络安全监测服务 | 对单位进行7\*24小时监测（含互联网）。针对业主方打造的 SaaS 应用，协助业主方管理全单位资产及风险的 SaaS 化订阅服务。可实现对单位的IP、端口、服务、漏洞、安全风险、违规内容、不合规资产等进行周期性监控，支持多维度分析单位安全等级。利用可视化性能数据、告警通知、量化的评分机制，帮助管理员了解安全态势，及时收敛攻击面，处理违规事件，减少安全隐患，降低通报风险。人员要求：供应商投入本项目团队人员至少具有2名人员获得IT 控制框架 COBIT 认证能力证书（提供资质复印件并加盖投标人公章）。服务频率：7\*24小时。 | 1年 |  |
| 9 | 应急响应服务 | 当发生外部黑客入侵、数据泄露、木马病毒等突发安全事件时，提供7\*24应急服务。服务内容包括事件检测与分析、风险抑制、问题根除、协助业务恢复等服务，最大化降低安全事件带来的影响。1、网络安全事件范围包含：web安全事件、恶意程序事件、网络攻击事件、信息破坏事件。2、应急服务工作开展范围：（1）招标人单位确实发生了第“1”条中列举范围内的重大网络安全事件，根据招标人单位已有的或我单位事先制定好的《网络安全事件应急预案》进行应急响应处置。（2）互联网上暴露出的核弹级重大漏洞（如：log4j、spring cloud function RCE），需要紧急自查。（3）应急响应成功处置后必须进行残留风险横向排查，防止其他主机遭受本次事件的影响。服务频率：一年内按需执行。交付材料：《网络安全事件响应处置报告》 | 1年 |  |
| 10 | 下属集团合规检查 | 1.根据提供的企业清单，开展企业现场网络信息安全和数据保护评估测试，评估内容包括但不限于企业网络信息安全防护能力、数据分类分级管理、数据安全性保护能力等，以及重点被查系统的安全漏洞情况，通过现场评测够较为清晰地了解企业当前所面临的安全风险和重要信息系统的安全现状。协助单位对下属国有企业开展制度专项检查工作，主要对《网络安全法》《个人信息保护法》《数据安全法》及网络安全工作责任制落实工作指标等工作制度检查。本项目为专业安全服务，供应商至少有一名具有工信部颁发的高级网络信息安全工程师并具有数据安全能力成熟度模型测评师（DSMM)资质证书。（提供资质复印件并加盖投标人公章）。2、服务范围：下属重点企业单位3、服务频次：1年不低于1次 | 1年 |  |
| 11 | 信息与网络安全管理平台 | 为满足招标人对安全服务的日常监督和管理，投标人提供SAAS云化安全监管类服务平台为招标人进行服务管理。需达到如下要求：A、系统需分配给招标人专业的账户密码，以方便业主方能够随时上传下载服务商的所有实施和服务材料。支持安全服务驾驶舱，展示各项服务开展进度，包括定级评估、安全运维、安全培训、安全评估、数据安全、安全运营等，为招标人提供服务决策（提供证明截图并加盖投标人公章）。B、支持项目内容管理：包含所有服务完成情况、服务期限、服务工单等基本信息查看（提供证明截图并加盖投标人公章）。C、同一个用户多个项目，要求能够展示所有项目数据。D、提供国家版权局颁发的《计算机软件著作权登记证》。（提供资质复印件并加盖投标人公章）E、用户数据全流程加密，安装专用加密软件环境，确保用户数据安全。 | 1年 |  |
| 12 | 国产化防火墙 | 1. 使用国产化硬件及自研软件系统；（需提供芯片厂商盖章的产品适配证明）2、硬件规格：1U，2个USB端口，1个Console端口。千兆电口≥10个，千兆光电复用接口≥4个，Bypass≥3组，内存≥4GB，提供额外可扩展插槽≥2个（最多支持不小于30个千兆电口，最多支持不小于12个千兆SFP光口，最多支持不小于4个万兆SFP+光口， 最多支持不小于3对Bypass端口），内置双交流电源，配置独立的日志存储盘≥1T SATA硬盘；3、性能规格：网络吞吐量不小于12G，并发连接数不小于400万，新建连接数不小于10万。4、NAT功能：支持IPv4/IPv6源NAT、目的NAT、静态NAT；支持跨协议NAT转换：NAT64、NAT46，具备IVI、嵌入地址、地址池三种转换形式；5、安全策略：支持基于IPv4/IPv6的一体化安全策略：在一条策略中可基于设备接口/安全域、源/目的IP地址、服务、应用、用户、时间等属性，配置工业防护、入侵防护、病毒防护、Web访问策略、应用控制等安全防护功能；支持IPv4/IPv6策略分析功能，支持检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略，并提供优化建议及图形化分析统计。（必须提供产品截图）6、支持OPC\_UA、OPC\_DA、S7、S7 PLUS、MODBUS、IEC104、DNP3、ENIP\_IO、ENIP\_TCP、ENIP\_UDP、MMS 等工控协议的读写控制。7、★防暴力破解：支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、postgres、mysql等常见协议的防暴力破解功能，针对每种协议可自定义检测时长和阈值，并自动将攻击者加入黑名单。

8、系统集成风险扫描功能：支持IPv4/6网络下telnet、ssh、ftp、imap、pop3、smtp、mysql、postgresql、mssql、rlogim、vnc等常见协议的弱密码检测功能，支持快速扫描、全面扫描、自定义扫描、空密码、用户名和密码相同等检测方式，弱口令字典可自定义设置。（必须提供产品截图）9、支持DoS/DDoS攻击防护、暴力破解防护等多种安全防护策略，支持工业协议深度防护功能，对工业协议定义白名单访问控制，对主流工业协议的功能码、线圈值、地址范围等进行深度检测实现过滤和防护；提供IPsec、SSL、GRE多种VPN Overlay，可支持HA、VRRP冗余组网，可开通支持扩展入侵检测防护功能，可针对目录遍历、蠕虫病毒、木马后门、跨站攻击、SQL注入、漏洞扫描等多种类型攻击行为进行检测防护；支持扩展病毒检测防护功能，针对主流网络协议、主流文件类型进行恶意代码检测防护；支持扩展七层应用识别和WEB站点分类识别，提供应用流量分析、网络访问审计、智能流量控制、网络行为管理等功能。10、含三年基础硬件保修系统软件维保服务，三年病毒、入侵防御、URL分类、应用特征库升级。 | 3套 |  |
| 13 | 终端安全监管平台 | 1.产品采用控制端+客户端架构，通过统一控制中心实现对各客户端统一策略下发、运行管理、全网健康状态监测、统一杀毒等、统一补丁功能；客户端授权数量：≥170个PC客户端授权（信创PC客户端）。2.支持信创/非信创环境客户端同一控制中心统一纳管及策略下发（含杀毒及其他终端安全管理能力）（提供功能截图）；3.支持对单个客户端进行维护，终端视角查看终端基本信息，包括计算机名、型号、IP、MAC地址、工作组、域信息、本次开机时间、上次关机时间、应用功能、在线状态、资产品牌、设备出厂日期；硬件信息展示，包括CPU、主板、内存、磁盘存储、显卡、显示器、声卡、网卡等信息；实时进程信息展示，包括进程名称、PID、进程用户名、命令行、占用内存、CPU占用、MD5等信息；网络信息展示，包括IP获取方式、IP地址、子网掩码、默认网关、DNS等信息；4.管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性；5.支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理中心；6.支持不少于两个杀毒引擎混合使用，提高病毒检出率；（提供功能截图） | 1套 |  |
| 14 | 内容及播控安全防护平台 | 1. 终端支持对接入的公共显示屏播放内容进行AI智能检测审核、事中控制，阻断不良信息播放，并将检测到的违规内容信息报送至平台。
2. AI智能检测审核：在视频、文字、图片等播放内容传输到公共显示屏前，先经过公共显示屏内容安全智能审核设备进行检测审核。
3. 事中控制：终端支持24小时不间断检测显示内容，当检测出播放内容中包含：涉黄、涉暴恐、涉政旗帜、敏感人脸、敏感词、涉毒、涉赌等视频或图像时，立即将播放内容替换为预设画面（即自定义安全图片）进行播放，阻断不良信息播放，待检测出播放内容合法合规时，可自动恢复内容输出，同时终端向平台提供违规事件统计、事件查询、事件详情等完善的审计溯源日志并可生成报表；（需提供具有CMA或ilAC-MRA或CNAS标识第三方权威检测机构出具的检测报告复印件，报告编号在检测机构官网可查询并提供截图和网站链接证明，报告首页带二维码以备现场查验）
4. 终端应具备防入侵、防篡改能力，确保终端系统不被篡改和破坏；
5. 为确保终端通信的可靠性、告警信息的精准性，终端支持与系统时间同步，时间同步精准至秒。（提供软件功能截图佐证）
6. 支持配置屏蔽持续时间：系统可自定义出现告警时，屏蔽预置图的持续时间。配置时间范围：0.1秒到86400秒（24小时），屏蔽持续时间为0时，则不会自动恢复，画面处于持续屏蔽状态。
7. 接口配置：≥1\*TYPE-C接口，≥1\*DP接口，≥1\*USB3.0接口，≥2\*USB2.0接口，≥2\*HDMI接口，≥2\*LAN口，≥2\*Wifi天线；信号灯配置：≥1\*WIFI信号灯，≥1\*网络信号灯，≥1\*PWR信号灯；支持RS485及RS232；（提供实物照片佐证）
8. 终端应能满足在不低于50000次识别敏感人脸视频或图像测试中，识别准确率≥99.99%；（需提供具有CMA或ilAC-MRA或CNAS标识第三方权威检测机构出具的检测报告复印件）
9. 终端应能满足在不低于50000次正常图像测试中，图像中均无敏感人脸视频或图像信息，误识别率≤0.01%；
10. 终端主机安全测试中，产品不应存在已知高、中风险等级的终端主机安全脆弱性问题。
11. 终端主机支持信息系统安全审计产品应将审计记录和自身审计日志存储于掉电非易失性存储介质中。
12. 信息系统安全审计产品不应提供对数据进行添加、修改、删除的功能或接口，防止审计记录和自身审计日志被篡改；
13. 管理平台集合了各类告警数据、违规视频预览、设备状态管理等多项关键数据和分析报告，并通过图表、仪表盘等各种视觉化工具，帮助用户快速监控业务变化并作出相应决策。
14. 管理平台支持多节点终端接入，对接入的终端所检测到的不良内容信息集中汇总管理与处置。
15. 支持多台设备接入云平台批量管理，平台首页支持查看接入设备总数、在线/离线设备数、告警信息、告警统计、告警类型、趋势统计；
16. 支持模型升级管理，模型升级管理需包含模型列表和版本列表两个部分。模型列表支持包括：涉黄识别、暴恐识别、特殊旗帜识别、人物库识别及敏感词识别；版本列表支持新增、编辑、删除以及启用/禁用的操作，版本列表支持显示版本名称、当前版本号及上一个版本。可通过搜索版本名称，搜索出相应的模型版本。（需提供软件截图证明）
17. 支持对设备远程下发操作，包括关屏、复位、重启设备、关闭检测功能；（需提供软件截图证明）
18. 支持对当前处于画面屏蔽状态的大屏进行画面复位操作，点击复位按钮，大屏画面从阻断状态恢复为可正常播放状态。
19. 终端支持执行关闭检测功能，特殊场景需求时，支持将终端检测功能暂时关闭，此时将不会对播放内容进行检测与屏蔽；
20. 支持应急联系人管理功能，支持管理各设备分组的应急联系人；（需提供软件截图证明）
 | 1套 |  |
|  | 合计 |  |  |  |