贵州省无线电管理信息系统网络安全建设项目

采购文件

项目编号：P52000020250006JB

采　　购　　人：贵州省无线电监测站

采购代理机构：大成工程咨询有限公司

日　　　　期：2025-07-08

第一章　采购公告

项目概况

贵州省无线电管理信息系统网络安全建设项目 招标项目的潜在投标人应在贵州省公共资源交易中心网上获取（交易中心网址：http://ggzy.guizhou.gov.cn/） 获取招标文件。并于 2025 年 7 月 30 日 09：30 时 （北京时间）前递交投标文件。

一、项目基本信息

项目名称：贵州省无线电管理信息系统网络安全建设项目；

项目编号：DCZX25-GZ-招标 A021；

采购方式：公开招标；

项目序列号：P52000020250006JB ；

采购主要内容：涵盖贵州省无线电监测站主中心节点与备份中心节点的核心交换机、汇聚交换机、接入交换机、超融合服务器、超融合软件、出口边界防火墙、核心业务边界防火墙、病毒过滤网关/防毒墙、网络准入控制、WEB 应用防火墙、运维安全审计/堡垒机、数据库审计、全威胁检测系统和态势感知平台、日志审计、无线电管理平台防护系统、漏洞扫描、VPN 等货物的采购、安装、本机调试、联网调试等集成服务内容，包括二次深化设计、包装及运输、出厂检验、到货验收、分部验收、单位验收、试运行、合同项目完成终验、质保、巡检、故障响应、维保、备品备件供应、技术培训、安全管理体系支

撑服务、安全运行体系支撑服务等技术服务内容；具体详见第五章采购需求；

本项目由贵州省无线电监测站实施招标采购，供应商中标后持中标通知书与贵州省无线电监测站签订合同，并按招标文件、投标文件和合同要求完成项目实施和资金支付。

采购数量：1批；

预算金额：2700000.00元；

最高限价：2640000.00元；（**（主中心节点）设备最高限价215万；备份中心节点最高限价29万元；集成费最高限价20万元**）

本项目（是/否）接受联合体投标：否

二、申请人的资格要求：

（1）一般资格要求：供应商符合《中华人民共和国政府采购法》第二十二条规定，并按招标文件要求规范提供下列材料（需加盖供应商公章）。

①具有独立承担民事责任的能力：提供法人或者其他组织的营业执照等证明文件，自然人的身份证明。

②具有良好的商业信誉和健全的财务会计制度：供应商是法人的，应提供2023年度(或2024年度)经审计的财务报告或基本开户银行出具的2025年的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具的2025年的资信证明。

③具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的证明材料或承诺函。

④有依法缴纳税收和社会保障资金的良好记录：提供2025年1月至今任意三个月缴纳税收的凭据或证明材料复印件(依法免税的供应商须提供相应证明文件)及2025年1月至今任意三个月社会保障资金缴纳证明材料复印件(不需要缴纳社保资金的供应商须提供相应证明文件)。

⑤参加本次政府采购活动前三年内在经营活动中没有重大违法记录：提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明或承诺函。

⑥.法律、行政法规规定的其他条件：供应商需提供承诺函：承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果。

⑦本项目不接受联合体

（2）特殊资格要求：无

三、获取招标文件

时间：2025年07月 09 日 至 2025年07月16日,每天上午00:00至11:59 ，下午12:00至 23:59（北京时间，法定节假日除外）

地点：贵州省公共资源交易中心网上获取（交易中心网址：https://ggzy.guizhou.gov.cn/）

方式：贵州省公共资源交易网->网上交易大厅->文件下载板块

（交易中心网址 ：https://ggzy.guizhou.gov.cn/）

售价（元）：0

四、提交投标文件截止时间、开标时间和地点

截止时间： 2025 年 07 月 30 日 09 时 30 分 （北京时间）

投标地点（网址）：贵州省公共资源交易中心网（交易中心网址：https://ggzy.guizhou.gov.cn/）

开标时间： 2025 年 07 月 30 日 09 时 30 分

开标地点：贵州省公共资源交易中心

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

采购项目需要落实的政府采购政策：《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）、《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19 号）、《关于政府采购支持监狱企业发展有关问题的通知》(财库〔2014〕68 号)、《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）、《关于进一步落实政府采购有关政策的通知》（黔财采［2014］15 号）。

PPP 项目：否

简要技术要求、服务和安全要求：具体要求详见招标文件

交货地点或交货期：/

服务期：在合同签定后待收到甲方开工令之日起 90 个日历天安装完成建设调试。服务地点：采购人指定地点。

其他事项（如样品提交、现场踏勘等）：现场踏勘 2025 年 07 月 18 日 9：00-11:30

七、对本次招标提出询问，请按以下方式联系

1.采购人信息

名 称： 贵州省无线电监测站

项目联系人： 俞老师

地 址： 贵阳市瑞金南路 58 号君悦华庭 B 栋 7 楼

联系方式：0851-85250049
2.采购代理机构信息
名　称：大成工程咨询有限公司
联 系 人：　罗在敏、曹飞、杨剑、孟宇
地　址：贵阳市观山湖区六盘水路启林创客小镇 D 栋 2 楼
联系方式：15761686763
3.项目联系方式
项目联系人：罗在敏、曹飞、杨剑、孟宇
电　话：15761686763

省公共资源交易中心电子招标远程开标须知

一、关于开标程序

本项目采用电子招标远程开标，供应商无须到现场递交投标文件和参加开标会议。

1. 开标准备：供应商应在投标截止时间之前使用数字证书（实体CA锁或贵州交易通APP）自行登陆远程开标系统，根据系统检测提示完成开标电脑环境配置。（环境配置及加解密注意事项详见：https://ggzy.guizhou.gov.cn/fwzn/xzzx/czsc/）

2.出现下列情形之一，将予以拒收投标文件：①投标截止时间前未完整上传；②未按规定进行电子签名、加密。③投标截止时间前未交纳投标保证金。

3.投标文件远程解密：在解密前采购人（代理机构）对递交的纸质保函真伪进行验证，验证未通过的视为投标保证金交纳不成功，不得参加解密。在采购人（代理机构）发出解密指令后，供应商应使用加密投标文件的数字证书（实体CA锁或贵州交易通APP），在代理机构设置的时间内完成解密。如因供应商网络问题、访问设备终端问题、未按操作手册要求完成设备环境设置或检测、解密数字证书发生故障或用错等，导致投标文件未在规定时间内完成解密，视为无效投标文件。

（环境配置及加解密注意事项详见：https://ggzy.guizhou.gov.cn/fwzn/xzzx/czsc/）

4.开标结果确认：供应商在**解密完成**后，应对**投标**内容进行确认，确认时间为 10 分钟。未在规定时间内对**投标内容**进行确认且未提出异议（质疑）的，视为默认开标结果。

5.公开开标信息：确认投标信息后，系统生成开标记录表，内容包含所有投标人名称和招标文件规定的其他内容，并将开标记录表在网上开标系统内公开。

6.供应商如发现系统提取的自身投标信息不正确的，可通过远程开标系统向采购人（代理机构）提出异议。

二、关于投标文件递交方式及要求

本项目为电子招标远程开标项目：供应商须在递交投标文件截止时间前完整的将加密电子投标文件（.GPT对应格式）上传到全国公共资源交易平台（贵州省）（网址：ggzy. guizhou.gov.cn ），加密上传的电子投标文件最大不超过500MB。投标截止时间前未完成投标文件传输或撤回投标文件的，视为未递交投标文件。**投标截止时间后，贵州省公共资源交易平台不再接收投标文件。**远程开标需使用数字证书（实体CA锁或贵州交易通APP）进行远程解密，解密证书必须是生成投标文件时使用的加密数字证书。

公示期结束后，中标人须按招标人要求提交与电子投标文件一致的纸质投标文件。

三、关于异常情况处置

出现下列情形之一的，暂停项目开标，并根据实际情况向监督部门报告：

1. 交易系统发生服务器故障、业务系统故障、数据库故障等，导致无法正常访问网站或无法正常使用交易系统；

2. 受到网络攻击或发生安全漏洞等问题，导致交易系统有潜在泄密风险；

3. 发生计算机病毒，导致交易系统无法正常运行；

4. 发生电力或网络故障，导致交易系统无法运行；

5. 其他非投标人原因，导致开标无法正常进行。

若发生的故障在三个小时内排除，则重新启动项目开标；若三个小时内未排除故障，则另行通知开标时间。

四、关于注意事项

1.电子招标远程开标会议期间，供应商均应在开标设备旁，直至开标结束，如因不能及时响应或反馈导致出现问题的供应商自行承担。

2.供应商参加电子招标远程开标项目，应在投标截止时间前完整上传经过数字证书（实体CA锁或贵州交易通APP）加密的投标文件。

3.供应商应提前完成数字证书的检查，确保参与本次投标活动中使用的数字证书与加密投标文件的数字证书为同一证书（实体CA锁或贵州交易通APP绑定的移动证书），确保开标过程中可正常在线进行投标文件解密、确认报价、开标异议等网上交互相关操作。（环境配置及加解密注意事项详见：https://ggzy.guizhou.gov.cn/fwzn/xzzx/czsc/）

4.投标文件**加解密**只能始终选择实体CA证书（实体CA锁）或移动CA证书（贵州交易通APP）其中一种方式，在交易活动过程中不能交叉操作使用。

注：贵州交易通APP的注册办理及咨询，可拨打官方服务热线：400-658-7878，操作手册下载地址：https://service.ebidsun.com/#/activity/guizhou）

5.请早于项目开标时间1天登录贵州省公共资源交易平台，使用平台提供的环境检测工具进行开标环境检测（实体CA锁检测地址：

https://ggzy.guizhou.gov.cn/hallweb/open-web/#/detection, 移动CA证书（贵州交易通APP）检测地址：https://service.ebidsun.com/#/activity/guizhou/check）。

6.开评标全过程中，供应商参与远程交互的人员应始终为同一人，若随意更换自行承担由此导致的一切后果。

7.因供应商使用的操作终端（软件或硬件）发生故障或参数设置等问题，导致不能参与交易活动，由供应商自行承担一切后果。

8.供应商在开标过程中操作遇到问题时，请及时向贵州省公共资源交易中心咨询。

（咨询电话：0851-85971671/85971629；QQ群：530035634 贵州交易通服务热线：400-658-7878 QQ群：597556561）

（如采购文件中其他章节关于远程开标描述与本须知不一致的以本须知为准）

第二章　供应商须知前附表

序号	内　　容	说 明 与 要 求
1	项目名称	贵州省无线电管理信息系统网络安全建设项目
2	供应商资格要求	（1）一般资格要求：供应商符合《中华人民共和国政府采购法》第二十二条规定，并按招标文件要求规范提供下列材料（需加盖供应商公章）。 ①具有独立承担民事责任的能力：提供法人或者其他组织的营业执照等证明文件，自然人的身份证明。 ②具有良好的商业信誉和健全的财务会计制度：供应商是法人的，应提供2023年度(或2024年度)经审计的财务报告或基本开户银行出具的2025年的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具的2025年的资信证明。 ③具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的证明材料或承诺函。 ④有依法缴纳税收和社会保障资金的良好记录：提供2025年1月至今任意三个月缴纳税收的凭据或证明材料复印件(依法免税的供应商须提供相应证明文件)及2025年1月至今任意三个月社会保障资金缴纳证明材料复印件(不需要缴纳社保资金的供应商须提供相应证明文件)。 ⑤参加本次政府采购活动前三年内在经营活动中没有重大违法记录：提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明或承诺函。 ⑥.法律、行政法规规定的其他条件：供应商需提供承诺函：承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果。 ⑦本项目不接受联合体 （2）特殊资格要求：无
3	投标保证金	1.投标保证金金额：¥20,000.00元。 2.投标保证金交纳形式:：以银行转账、保证保险、银行保函或合法担保机构出具的担保等非现金形式提交（详细按照贵州省公共资源交易中心规定执行）。。 3.投标保证金的有效期同投标有效期。

		4.投标保证金交纳截止时间：按采购公告的规定办理。 5.投标保证金交纳要求详见本文件的第三章第三节。	
4	投标报价	投标报价应包括：（1）报价不得高于本项目最高限价。 （2）报价方式为包干价。 （3）报价中包含人员的劳动报酬、福利待遇、按法规交纳社会保险、残疾金、工伤抚恤、公积金、商业保险、服务费、管理费、交通费、培训费、员工服装及配备费等各项费用、税费、成交服务费、合理利润、风险费用及合同签订过程中可预见和不可预见费用等。（4）投标（响应）供应商需自行考虑本项目在实施期间的一切可能产生的费用。在合同执行过程中，采购人将不再另行支付与本项目相关的任何费用（非本项目要求的其它内容除外）。（5）投标货币：人民币。	
5	投标文件的递交	本项目为电子招标不见面开标项目：供应商须在递交投标文件截止时间前完整的将加密电子投标文件（.GPT 对应格式）上传到全国公共资源交易平台（贵州省）（网址：ggzy.guizhou.gov.cn ），投标截止时间前未完成投标文件传输或撤回投标文件的，视为未递交投标文件。投标截止时间后，贵州省公共资源交易平台不再接收投标文件。 远程开标需使用数字证书（实体 CA 锁或贵州交易通 APP）进行远程解密，解密证书必须是生成投标文件时使用的加密数字证书。 公示期结束后，中标人在领取中标通知书时须按招标人要求提交与电子投标文件一致的纸质投标文件。	
6	开标	时 间	见采购公告
		地 点	贵州省公共资源交易中心（具体标室详见开标当天交易中心开标区大屏幕）
7	评 标	评标方法	综合评分法
8	服务要求	1.服务期：在合同签定后待收到甲方开工令之日起 90 个日历天安装完成建设调试。2.服务地点：采购人指定地点。	
9	质保期	三年(具体延保服务时限以投标文件为准)，包括所有软、硬件系统设备。质量保修期内，对于非人为因素造成的故障及损坏，予以全包免费维修保养；质量保修期从产品安装、调试完毕之日算起，乙方须提供长期稳定的技术支持，并及时为甲方解决技术问题；	
10	付款方法和条件	合同签订后 30 个日历日内，采购人支付合同金额的 40%作为预付款；项目合同验收合格后 30 个日历日内，采购人支付合同金额的 50%（支付前，中标人须提供银行出具的与预付款等额的预付款保函，保函期限为 1 年）；项目初步验收合格后 30 个日历日内，采购人支付合同金额的 10%；中标人完成竣工验收后,采购人按规定办理银行保函退还相关手续(付款前甲方有权	

		组织抽查，如发现产品质量或售后服务有问题且未得到及时处理的，甲方有权拒绝付款)。 注:1.以上付款均不计利息，乙方须执行财政支付流程及管理办法，并在甲方付款时须提供足额有效的专用发票，因乙方票据提供不及时，以及不符合税务机关相关要求，而导致合同款不能支付的责任由乙方承担。付款方式为转账、电汇或保函等，具体方式由甲方根据实际情况而定。若采购人逾期付款的应按照逾期付款金额的银行同期活期利率支付逾期付款违约金，但违约金总额不超过应付款金额的 10%。
11	**履约保证金**	为保证合同的顺利执行，乙方必须在与甲方签订合同前，向甲方提交金额为中标总价 10%的履约保证金，逾期未提交履约保证金作自动放弃中标处理。 2、履约保证金应当以支票、汇票、本票或者保险公司、金融机构、担保机构出具的保函等非现金形式提交。提交形式由乙方自主选择，甲方应按规定接受乙方提交的保证保险。 3、如乙方未能履行合同规定的义务，甲方有权从履约保证金中取得补偿。 4、履约保证金在合同约定期间内不予退还或者应完全有效，约定期间届满之日起 20 个工作日内，甲方应将履约保证金退还乙方；逾期退还的，按中国人民银行同期贷款基利率上浮 20%后的利率支付超期资金占用费，但因乙方自身原因导致无法及时退还的除外。 5、履约保证金在项目验收合格后退还给乙方。
12	**质疑**	供应商须在法定质疑期内一次性提出针对同一采购程序环节的质疑。
13	招标代理服务费	一、收费标准 代理机构严格遵守《价格法》《关于商品和服务实行明码标价的规定》等法律法规规定，告知有关服务项目、服务内容、服务质量，以及服务价格等，并在相关服务合同中约定。代理机构提供的服务，应当符合国家和行业有关标准规范，满足合同约定的服务内容和质量等要求。不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。 代理服务费收费标准：参考国家计委计价格[2002]1980 号文件，以中标供应商的中标价为基数计算后下浮向中标供应商收取代理服务费，并由中标供应商在领取中标通知书时支付给乙方。 二、支付方式 中标供应商在领取中标通知书时，向代理机构支付中标服务费及评审专家费。中标服务费可采取现金、银行汇款、电汇款或其他代理机构认可的方式进行支付。 三、账户信息 户　　名：大成工程咨询有限公司贵州分公司

		开户银行：中国银行股份有限公司贵阳市东山支行 帐　　号：133035419075 **注：此账户非投标保证金缴纳账户。**
14	发布公告的媒介	贵州省政府采购网、全国公共资源交易平台（贵州省）等网站法律法规规定的其他媒体
15	政府采购合同备案	根据《政府采购法》第四十六条和《政府采购法实施条例》第五十条的有关规定，成交供应商在成交通知书发出之日起 30 天内必须与采购单位签订《政府采购合同》，在合同签订 2 个工作日内将合同扫描件送至采购代理公司，由采购代理机构发布合同公告。如成交供应商未能按以上规定时间办理，造成的所有后果自负。
16	**其它**	1、如投标文件中有英文或其它语种时，请翻译成中文。本项目部分产品接受进口产品投标。 2、其他责任： (1) 乙方须承诺，项目建设及服务期、延保服务期内，因在工作中引起各种工伤、安全事故、事故责任由乙方自行承担，与甲方无关，甲方不承担任何责任和经济赔偿。 (2) 乙方在项目建设过程中，非因甲方原因造成工期延误的，一律由乙方承担，产品设备投标选型不正确造成施工中产品变更，甲方将追究其责任

第三章　供应商须知正文

一、供应商须知正文

第一节 发布采购公告

一、公告发布媒体

贵州省政府采购网、全国公共资源交易平台（贵州省）等网站及法律法规规定的其他媒体。

二、变更公告

本项目将根据实际情况及需要，发布技术参数、延长投标截止时间和开标时间等有关内容的变更公告。供应商须关注贵州省政府采购网、全国公共资源交易平台（贵州省）等网站及法律法规规定的其他媒体关于本项目的变更公告。变更公告是招标文件的组成部分，与招标文件具有同等法律效力。

第二节 获取招标文件

一、获取时间

以本项目公告时间为准。因特殊需要推迟开标时间的，采购人或采购代理机构应当在贵州省政府采购网、全国公共资源交易平台（贵州省）等网站及法律法规规定的其他媒体上发布变更公告，参与投标的供应商应自行关注。

二、获取方式

以本项目公告中获取方式为准。

三、招标文件的澄清和修改

（一）采购人或者采购代理机构可以对已发出的招标文件进行必要的澄清或者修改。澄清或者修改的内容可能影响投标文件编制的，采购人或者采购代理机构应当在投标截止时间至少 15 日前，以发布更正公告形式通知所有获取招标文件的潜在供应商；不足 15 日的，采购人或者采购代理机构应当顺延提交投标文件的截止时间。补充变更文件是招标文件的组成部分，对所有供应商均具有约束力。所有招标文件的补充、变更将以更正公告形式发布。

（二）采购人延长投标截止时间和开标时间应在招标文件要求提交投标文件的截止时间 3 日前，将变更时间以发布公告形式形式所有招标文件收受人。

（三）潜在供应商或其他利害关系人对招标文件有异议的，应公告期限获取招标文件之日起七个工作日内或采购公告期限后获取招标文件的，在采购公告期限届满之日起七个工作日内向采购人或代理机构书面提出。

招标文件质疑、投诉的具体要求和流程详见招标文件第七节：发布中标公告，第二点：政府采购活动的质疑投诉。

第三节 交纳投标保证金

一、是否交纳保证金：

是 ☑ 否 □

二、交纳金额：20000.00 元

三、投标保证金交纳要求

1.投标保证金收取（到账）截止时间：详见本项目招标公告要求（温馨提示：为确保保证金缴纳成功，建议您在保证金缴纳截止时间前 1 个工作日的 16:00 前完成保证金绑定）。

2.投标保证金缴纳和退还按贵州省公共资源交易中心相关规定办理，缴纳保证金的流程（详见 http://ggzy.guizhou.gov.cn/fwzn/xzzx/czsc/202008/t20200820_62579611.html，“2020 版交易系统保证金操作手册”）。

3.投标保证金交纳方式：银行转账 保证保险 银行保函 合法担保机构出具的担保

3.1 银行转账形式提交投标保证金

（1）贵州省公共资源交易系统 2020 版以银行转账方式交纳的投标保证金，须由供应商在投标截止时间前自行在系统内与投标项目进行绑定。

（2）在交纳保证金前，请先在交易系统的“企业诚信管理系统—企业基本信息—银行账户”下验证“开户银行、基本账户号、基本户开户支行号、基本户账户名称”等信息是否正确完善。检查完毕后，通过基本账户将保证金转入贵州省公共资源交易中心保证金账户。

开户名称：贵州省公共资源交易中心

开 户 行：贵州银行股份有限公司贵阳展览馆支行

账 号：0109001400000182-0002

支 行 号：313701099123

（3）保证金转账成功后登陆交易系统，点击【保证金管理】菜单下的【交纳流水查看】，查看该笔保证金是否鉴收成功。

（4）保证金鉴收成功后，点击【项目绑定】菜单中绑定投标项目，点击【绑定】按钮，绑定成功后保证金方可生效。

（5）项目绑定成功后，点击【交纳凭证】按钮，可打印保证金交纳凭证。未绑定或未绑定成功的，视为未交纳投标保证金，不能参加投标。

（6）未绑定成功的保证金在 60 日内将自动进行退款。

3.2 银行保函、保证保险、合法担保机构出具的担保等方式提交投标保证金

（1）供应商通过贵州省公共资源交易综合金融服务平台在线办理的电子保函：包含银行保函、保证保险、担保保函等（注： 内容应载有招标人名称、供应商名称、项目名称、标段名称、投标保证金金额、有效期（应不小于投标有效期），可直接在交易系统中确认，须将打印的电子保函和投标文件一并提交给招标代理机构，不再验证真伪。

（2）对贵州省公共资源交易综合金融服务平台以外办理的投标保函（含纸质保函）、合法担保机构出具的担保，须将电子保函原件和投标文件一并提交给招标代理机构，并在开标现场对其进行真伪验证，通过官网查询验证未通过的，视为未按规定交纳投标保证金。

第四节 递交投标文件

一、递交时间

以本项目公告时间为准，如本项目有变更公告的，以变更公告时间为准（供应商须在递交文件截止时间前递交密封的投标文件,代理机构工作人员对递交的投标文件进行登记并给予接收回执。不接受逾时递交的投标文件）。

二、递交地点

上传到全国公共资源交易平台（贵州省）（网址：ggzy.guizhou.gov.cn ）

三、递交要求

本项目为电子招标远程开标项目:供应商须在递交投标文件截止时间前完整的将加密电子投标文件（.GPT 对应格式）上传到全国公共资源交易平台（贵州省）（网址：ggzy.guizhou.gov.cn ），投标截止时间前未完成投标文件传输或撤回投标文件的，视为未递交投标文件。投标截止时间后，贵州省公共资源交易平台不再接收投标文件。远程开标需使用数字证书（实体 CA 锁或贵州交易通 APP）进行远程解密，解密证书必须是生成投标文件时使用的加密数字证书。公示期结束后，中标人在领取中标通知书时须按招标人要求提交与电子投标文件一致的纸质投标文件。

投标文件递交截止时间后，在代理机构发出解密指令后，供应商应使用加密投标文件的数字证书（实体 CA 或贵州交易通 APP），在 30 分钟内完成解密。 如供应商网络问题、访问设备终端问题、未按操作手册要求完成设备环境设置或检测、解密数字证书发生故障或用错等，导致投标文件未在规定时间内完成解密，视为无效投标文件。

四、投标响应文件的补充、修改和撤回

（1）供应商在提交投标响应文件后，在投标截止时间前可对其投标文件进行补充、修改或撤回。

（2）投标补充或修改文件必需加盖供应商单位公章并注明“补充或修改投标文件”字样和标识项目名称、项目编号、项目序列号、单位名称信息，要求密封递交。

（3）投标文件撤回必需在投标截止时间前提交由项目授权代表签署的撤回投标文件的通知，招标代理机构可以退回其投标文件。

（4）投标截止时间以后不得补充、修改或撤回投标文件。

第五节 开标、资格审查

一、开标时间

以本项目公告时间为准。如发布变更公告的，以变更公告时间为准。

二、开标地点

贵州省公共资源交易中心（贵州省贵阳市遵义路65号，具体开标室于当日在贵州省公共资源交易中心开标区获取）

三、开标流程

（1）采购人或采购代理机构在投标人须知前附表规定的开标时间和开标地点组织公开开标，采购人和有关方面代表参加。

（2）开标时，开标流程以交易中心电子平台流程进行开标和唱标。

（3）未宣读的投标价格等实质性内容，评标时不予承认。

（4）投标人代表及有关人员在开标记录上签字确认。

（5）开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查。

四、资格审查

根据政府采购法律法规规定和招标文件的规定，对投标文件中的资格证明、投标保证金等进行审查，以确定投标人是否具备投标资格。

资 格 审 查 表

序号	资格要求 \ 供应商名称		供应商 1	供应商 2	供应商 3
1	经营资格审查	具有独立承担民事责任的能力：提供法人或者其他组织的营业执照等证明文件，自然人的身份证明。			
2		具有良好的商业信誉和健全的财务会计制度：供应商是法人的，应提供 2023 年度(或 2024 年度)经审计的财务报告或基本开户银行出具的 2025 年的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具的 2025 年的资信证明。			
3		具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的证明材料或承诺函			
4		有依法缴纳税收和社会保障资金的良好记录： 提供 2025 年 1 月至今任意三个月缴纳税收的凭据或证明材料复印件(依法免税的供应商须提供相应证明文件)及 2025 年 1 月至今任意三个月社会保障资金缴纳证明材料复印件(不需要缴纳社保资金的供应商须提供相应证明文件)。			
5		参加本次政府采购活动前三年内在经营活动中没有重大违法记录：提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明或承诺函。			
6		法律、行政法规规定的其他条件： 供应商需提供承诺函：承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一			

		切法律责任及后果。			
7	联合体审查	本项目不接受联合体投标			
资格审查结论（通过或不通过）					

注：未通过资格审查的供应商，资格审查小组应现场告知未通过原因，且由供应商在资格审查表上签字确认同意资格审查结果，供应商如有异议，资格审查小组将现场予以复核一次。若供应商拒绝签字确认，又不当场说明拒签理由的，视为同意资格审查结果。

第六节 评标

一、评标时间

以本项目公告时间为准，如本项目发布变更公告的，以变更公告时间为准。

二、评标地点

贵州省公共资源交易中心。

三、评标程序

（一）宣布评标纪律以及回避提示

（二）评标委员会推选出一名评标组长，由评标组长组织评标活动

（三）符合性审查：评标委员会依照《符合性审查表》所列内容对供应商进行符合性审查，审查通过的供应商进入下一评审环节。未通过符合性审查的投标文件不参与下一评审环节和中标候选人推荐。通过初步审查的供应商不足三家的，本项目作废标处理，评标工作结束。

商务、技术实质性检查：评标委员会审查投标文件是否对招标文件作了实质性响应，即投标文件是否满足或响应招标文件技术、商务方面的要求。技术符合性：投标产品的技术成熟性、适用性、性能、参数和规格等满足招标文件要求，无实质性负偏离、反对、设定条件或提出保留；商务符合性：质保、交货期、投标有效期、付款条件等符合招标文件要求；不低于成本报价，不高于采购预算价；投标文件的组成、投标文件的完整性和有效性等符合招标文件规定，无实质性负偏离、反对、设定条件或提出保留。

无效标检查：依照本招标文件无效标条款规定审查供应商是否为有效投标。

（四）投标人的技术与商务分由评标委员会根据其提交的投标文件按照本招标文件规定的评分标准评出后的算术平均值。评标委员会成员对投标人给予的技术商务分值与算术平均值的比值超过±30%（含 30%）时，该成员应对其评分作出说明，评标委员会其他成员和监督席不认可其说明时，该评分无效。投标人的报价分将由投标文件中填报的投标报价按照本招标文件规定的计算方法计算获得；综合分为投标人的技术与商务分与报价分之和。

（五）评标委员会根据投标人评审得分高低排定名次。评标结果按评审得分由高到低顺序排列。得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的并列，投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分;汇总后评审得分由高到低的前 3 名为中标候选人。

（六）评审复核：评标委员会对评审过程和评审结果进行复核。评标委员会可对评审过程和结果中存在的遗漏或偏差进行修正，完成复核后，确定评标结果及推荐排序。

（七）评标报告：评标组长根据评标结果汇总情况及排序情况，主持编写评标报告。评标报告按规定需涵盖公告发布情况、开评标情况、推荐排序前三名中标候选人及有关需要说明的情况等政府采购法规规定的内容。评标委员会成员须在评标报告上签字确认。

（八）评标结束：评标委员会出具评标报告并复核无误后，由评标组长宣布评标工作结束。待代理机构工作人员收理好评标资料，并发放评审费用后评标专家方可离开评标区。评标过程中评标专家不得擅自离开评标区或进入其他评标室。

注：

（1）当初步审查结果确定有效供应商不足三家，或出现影响采购公正的违法违规行为，或供应商的报价均超过了采购预算采购人不能支付，或因重大变故采购任务取消的，或招标文件存在重大歧义、重大缺陷导致评审工作无法进行时，或招标文件内容违反国家有关规定的，评标程序终止。

（2）投标文件的评审和比较、中标候选人的推荐以及与评标有关的其他情况，评标委员会成员、采购人和采购代理机构等人员均不得泄露。

（3）开标、评标过程由贵州省公共资源交易中心全程同步录音录像，相关录音录像资料由贵州省公共资源交易中心存档，以便为财政、纪检监察等有关部门处理项目相关事宜提供资料。

（4）演示：如项目有演示需求的，由采购代理机构工作人员组织。

（5）评标过程中，如需出具统一意见但评标专家意见不一致的，按照少数服从多数的原则形成决议。

（6）评标结束后，采购人及采购代理机构依法对评标报告和推荐供应商的投标文件进行复核，发现投标文件内容真实性、符合性审查、评审结果等存在问题或错误的，可向原评标委员会提出协助答疑，或向省财政厅提请纠正。

四、评标委员会

评标委员会成员由采购人代表和有关技术、经济等方面的专家组成，其中技术、经济等方面的专家不少于成员总数的三分之二。评标委员会成员人数为单数。评标委员会遵循公平公正、科学择优、经济有效的原则，按照评标程序，依法依

规，根据招标文件所列评标标准，独立、认真、负责地开展评审工作，提出评审意见，并对自己的评审意见承担责任。

（一）享有的权利：

1、对政府采购制度及相关情况的知情权；

2、对供应商所供货物和服务质量的评审权；

3、推荐中标候选供应商的表决权；

4、按规定获得相应的评审劳务报酬；

5．法律、法规和规章规定的其他权利。

（二）承担的义务：

1、为政府采购工作提供科学合理、经济有效的评审意见；

2、严格遵守政府采购评审工作纪律，不得向外界泄露评审情况；

3、发现供应商在政府采购活动中有不正当竞争或恶意串通等违规行为，应及时向政府采购评审工作的组织者或财政部门报告并加以制止；

4、解答有关方面对政府采购评审工作中有关问题的咨询或质疑；

5、法律、法规和规章规定的其他义务。

五、询标与澄清

（一）评标过程中，评标委员会发现投标文件存在含义不明、表述不清、有歧义等情况，实质性影响评审结果的，评标委员会可书面向供应商进行询标，要求供应商对询问的问题进行澄清。供应商须在贵州省公共资源交易中心通知的时间内进行书面答疑和澄清。供应商未在通知的时间内进行答疑和澄清的，视为放弃澄清。

（二）供应商的答疑和澄清须为书面形式，须由供应商授权代表签字或加盖供应商公章。书面澄清文件为投标文件的组成部分。

（三）供应商对投标文件的澄清不得超出投标文件的范围或改变投标报价等实质性内容。澄清和补正应遵循公平公正的原则，供应商的澄清补正不得对其他供应商造成不公平不公正的结果或影响，如有，评标委员会应拒绝其澄清。

（四）供应商在投标文件中无需提供成本测算表，评标委员会认为其最终报价明显低于市场平均价格，存在异常低价的嫌疑时，要求供应商进行澄清时，需按附件要求提供成本测算表，按此进行成本的测算及澄清，并附上相应文字说明。

第七节 发布中标公告

一、公告发布媒体

贵州省政府采购网、全国公共资源交易平台（贵州省）等网站及法律法规规定的其他媒体。

采购代理机构应当自评审结束之日起 2 个工作日内将评审报告送交采购人。采购人应当自收到评审报告之日 起 5 个工作日内在评审报告推荐的中标或者成交候选人中按顺序确定中标供应商。采购人或者采购代理机构应当自中标供应商确定之日起 2 个工作日内，发出中标通知书。中标通知书对采购人和中标供应商具有同等法律效力。中标通知书发出后，采购人改变中标结果，或者中标供应商放弃中标，应当承担相应的法律责任。

二、政府采购活动的质疑投诉

（一）质疑

供应商认为招标文件、采购过程和中标、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日（政府采购法第五十二条规定的供应商应知其权益受到损害之日，是指：（一）对可以质疑的招标文件提出质疑的，为收到招标文件之日或者招标文件公告期限届满之日；（二）对采购过程提出质疑的，为各采购程序环节结束之日；（三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。）起七个工作日内，以书面形式向采购人提出质疑。

（二）受理条件

1、供应商所提出质疑，必需有认为招标文件、采购过程、中标和成交结果等使自己的利益受到损害的事实和依据，对与采购活动无关的供应商或者没有提出使自己的利益受到损害的事实和依据的质疑，可不予受理；

2、质疑必需以书面形式提出并署名，质疑人为法人或其他组织的，质疑书应当加盖质疑单位公章，以口头形式提出的，可不予受理；

3、在法定时间内提出质疑。供应商在认为招标文件、采购过程、中标和成交结果等使自己的利益受到损害后的七个工作日内提出质疑。

（三）质疑具体要求及注意事项：

1、质疑文件递交要求：质疑须以书面形式提出，列明质疑事项及相关依据，联系人、联系电话、传真、详细地址、邮编等基本信息。质疑函一式两份，加盖公章后，一份送本项目代理机构，一份送采购人处。除书面形式外，其他任何方式的质疑，采购人或代理机构不予以接受。

2、质疑文件递交地点：

代理机构：大成工程咨询有限公司

详细地址：贵阳市观山湖区六盘水路启林创客小镇 D 栋 2 楼

项目联系人：罗在敏、孟宇

电　　话：15761686763

3、供应商对招标文件质疑的截止时间为：供应商下载招标文件文件之日起 7 个工作日内。**供应商提供书面质疑文件的同时，向采购人或采购代理机构出示文件购买招标文件凭证的复印件并加盖公章。**

4、供应商须在法定质疑期内一次性提出针对同一采购程序环节的质疑。

5、质疑函的格式应遵照财政部发布的《政府采购供应商质疑函范本》进行填写，《政府采购供应商质疑函范本》下载网址：“中国政府采购网”（www.ccgp.gov.cn）。

（四）质疑答复：采购人或者采购代理机构应当在 7 个工作日内对供应商依法提出的询问作出答复。供应商提出的询问或者质疑超出采购人对采购代理机构委托授权范围的，采购代理机构应当告知供应商向采购人提出。政府采购评审专家应当配合采购人或者采购代理机构答复供应商的询问和质疑。答复内容不得涉及商业秘密。

（五）提出质疑的供应商对采购人或代理机构的答复不满意或采购人、采购代理机构在规定的时间内未作出答复的，可在收到答复之日起或答复期满后十五个工作日内向采购人同级政府采购监督部门投诉。

监督部门：贵州省财政厅政府采购监督管理处

联系地址：贵州省贵阳市中华北路 242 号省政府大院 7 号楼 312 室、308 室

联系电话：0851-86892180　　0851-86822706

第八节 支付代理服务费

一、收费标准

代理机构严格遵守《价格法》《关于商品和服务实行明码标价的规定》等法律法规规定，告知有关服务项目、服务内容、服务质量，以及服务价格等，并在相关服务合同中约定。代理机构提供的服务，应当符合国家和行业有关标准规范，满足合同约定的服务内容和质量等要求。不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

二、支付方式

中标供应商在领取中标通知书时，向代理机构支付中标服务费及专家评审。中标服务费可采取现金、银行汇款、电汇款或其他代理机构认可的方式进行支付。

三、账户信息

户　　名：大成工程咨询有限公司贵州分公司

开户银行：中国银行股份有限公司贵阳市东山支行

帐　　号：133035419075

注：此账户非投标保证金缴纳账户。

第九节 政府采购合同签订、备案及公告

一、签订、备案及公告时间

采购人与中标供应商应当在中标通知书发出之日起三十日内，按照招标文件确定的事项签订政府采购合同，采购合同自签订之日起七个工作日内，采购人应当将合同副本报同级政府采购监督管理部门和有关部门备案。

采购人应当自政府采购合同签订之日起 2 个工作日内，将政府采购合同在贵州省政府采购网上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

中标供应商拒绝与采购人签订合同的，采购人可以按照评审报告推荐的中标候选人名单排序，确定下一候选人为中标供应商，也可以重新开展政府采购活动。

二、合同内容

本项目拟签订的政府采购合同见第五章有关内容。中标供应商与采购人须按照本项目的招标文件和投标文件所载内容，及评标过程中有关澄清文件内容签订政府采购合同。

第十节 退还投标保证金

（仅适用于银行转账方式交纳投标保证金的供应商）

一、投标保证金的退还

1、投标保证金的退还方式以贵州省公共资源交易中心最新规定为准。

2、投标保证金的退还时间按财政部 87 号令的规定时间退还。

3、下列任何情况发生时，投标保证金将不予退还：

3.1 供应商有《中华人民共和国政府采购法》第七十七条所列行为的；

3.2 开标后在投标有效期间内，供应商撤回投标文件的；

3.3 除因不可抗力，中标供应商不与采购人签订合同的；

3.4 法律法规及招标文件规定的其他情形。

4、若发生质疑或投诉，与质疑或投诉有关的供应商的投标保证金有效期将延长，待质疑、投诉处理完毕之后予以办理。

5、根据财政部 87 号令的规定，采购人或者采购代理机构逾期退还投标保证金的，除应当退还投标保证金本金外，还应当按中国人民银行同期贷款基准利率上浮 20%后的利率支付超期资金占用费，但因投标人自身原因导致无法及时退还的除外。

6、满足投标保证金退款条件的投标保证金退还申请，在经贵州省公共资源交易中心财务核验通过后的第 T+2 个工作日到账，咨询电话：0851-85971671/85971629。

供应商保证金缴纳须知

投标保证金应以招标文件规定的交纳形式进行交纳，供应商可通过**贵州省公共资源交易综合金融服务平台PC端**或移动端（贵州交易通APP）在线办理电子保函（注：其内容应载有采购人名称、供应商名称、 项目名称、标段名称、保证金金额、有效期，且其有效期应不小于投标有效期），直接在交易系统中确认；未通过贵州省公共资源交易综合金融服务平台**交纳投标保证金的，应在交易系统中选择“纸质保函” 交纳方式，并上传保函扫描件，上传内容确保清晰可见。采购人（代理机构）在开标时对其进行真伪验证，通过上传保函中提供的在线官 网地址进行查验，检查未通过或不能查验的视为未按规定交纳投标保 证金。**

履约担保：需要提交履约担保的，可通过“**贵州省公共资源交易综合金融服务平台**“在线办理电子履约保函（银行保函、保证保险、担保保函）。登录交易大厅（https://ggzy.guizhou.gov.cn/hallweb/#/login）进入“**金融服务-电子保函及贷款**”即可办理，咨询电话：0851-85971629、0851-85971703。

报价与最高限价表

标包名称：贵州省无线电管理信息系统网络安全建设项目

序号	报价名称	报价形式	最高限价	报价单位	是否主报价	报价形式说明
1	贵州省无线电管理信息系统网络安全建设项目	金额报价	2640000.00	元	是	

开标一览表

项目名称：贵州省无线电管理信息系统网络安全建设项目　　项目编号：P52000020250006JB

（一）唱标记录

标包名称:贵州省无线电管理信息系统网络安全建设项目

序号	投标单位名称	贵州省无线电管理信息系统网络安全建设项目(元)	服务期	服务地点	签名
1					
2					
3					
4					
5					
6					
7					
8					

（二）开标过程中的其他事项记录

（三）出席开标会的单位和人员（附签到表）

招标人代表：_____ 记录人：_____ 监标人：_____ ____年____月____日

评标办法前附表

1、项目基本信息

项目编号：P52000020250006JB

项目名称：贵州省无线电管理信息系统网络安全建设项目

采购方式：公开招标

项目资金来源：财政资金

PPP项目：否

2、标包信息

标包1：贵州省无线电管理信息系统网络安全建设项目

基本信息

标包编号：P52000020250006JB001

标包名称：贵州省无线电管理信息系统网络安全建设项目

评标办法：综合评分法

是否考虑小微型企业价格扣除：是

是否考虑政策性加分：是

资格审查方式：资格后审

是否接受联合体：否

是否缴纳投标保证金：是

中标方法：推荐中标候选人

核心产品名称：

报价评审：有

预算金额(元)：2700000

评标步骤	序号	评审因素	评审标准	分值

评标步骤	序号	评审因素	评审标准	分值
资格性审查	1	具有独立承担民事责任的能力	提供法人或者其他组织的营业执照等证明文件，自然人的身份证明。	
	2	有良好的商业信誉和健全的财务会计制度	供应商是法人的，应提供2023年度(或2024年度)经审计的财务报告或基本开户银行出具的2025年的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具的2025年的资信证明。	
	3	具有履行合同所必需的设备和专业技术能力	提供具备履行合同所必需的设备和专业技术能力的证明材料或承诺函	
	4	有依法缴纳税收和社会保障资金的良好记录	提供2025年1月至今任意三个月缴纳税收的凭据或证明材料复印件(依法免税的供应商须提供相应证明文件)及2025年1月至今任意三个月社会保障资金缴纳证明材料复印件(不需要缴纳社保资金的供应商须提供相应证明文件)。	
	5	参加本次政府采购活动前三年内在经营活动中没有重大违法记录	提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明或承诺函。	
	6	法律、行政法规规定的其他条件	供应商需提供承诺函：承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果。	

评标步骤	序号	评审因素	评审标准	分值
	7	联合体审查	本项目不接受联合体投标	
符合性审查	1	投标保证金审查	提供保证金已交纳的依据。	
	2	商务实质性响应审查	满足招标文件第五章“第二节 商务要求”（无负偏离）。	
	3	技术实质性响应审查	无	
	4	报价审查	按本项目招标文件第四章 评标办法中第三节废标条款和第四节无效标条款的规定，审查是否通过。	
	5	授权委托	对授权人身份进行核验。	
商务评审	1	项目团队(满分5分)	本次项目要求投标安全产品制造商提供原厂实施服务，根据组建的项目团队进行评价：项目团队组织架构的完整性、项目成员的能力、管理等内容 1、项目实施人员每具备一个CISP证书或网络工程师证书得0.3分，最高得3分，不提供不得分； 2、投标人须固定一名售后服务人员(非项目实施人员），售后服务人员须同时具备CISP和ITSS证书得2分，提供1个得0.5分，不提供不得分。 注：项目实施人员组成可以是投标人、产品制造商人员组合，提供2025年1月至今任意1个月的社保缴纳证明材料。	5.00

评标步骤	序号	评审因素	评审标准	分值
	2	产品兼容性体现（满分10分）	1、投标产品无线电管理平台防护系统与我单位无线电管理一体化平台兼容性良好，能够持续、稳定的提供安全防护能力，对提供核心业务系统制造商出具的兼容性证明材料得7分(投标截止前三年内证明材料有效），不提供不得分。 2、投标产品态势感知平台（安全管理域）与我单位现有无线电监测终端安全防护系统联动处置安全事件兼容性良好，能够持续、稳定的提供网络安全事件联动处置能力，提供终端安全系统制造商出具的兼容性证明材料得3分(投标截止前三年内证明材料有效），不提供不得分。	10.00
	3	业绩（满分5分）	自2022年1月1日以来，投标人提供类似项目业绩，每提供一个得1分，最多得5分；需提供合同、项目竣工验收报告复印件并加盖投标人公章。 注：提供相关业绩合同关键页（关键页包括不限于首页、金额页、项目建设内容页、签字盖章页）复印件（加盖投标人公章），验收报告提供关键页（验收意见、签字页），不提供不得分。	5.00

评标步骤	序号	评审因素	评审标准	分值
技术评审	1	技术响应程度（满分40分）	提供产品的可销售证明（如销售许可证、商用密码产品认证证书、网络安全专用产品安全检测等）、性能参数、功能参数完全满足采购文件要求的40得分，标★的产品功能指标，需提供证明材料，（提供原厂参数确认函、截图证明材料并加盖原厂公章，参数中要求提供第三方测试报告的，只需要提供第三方测试报告，无需要提供参数确认函及截图。）否则视为负偏离。出现负偏离的，每项扣减3分，非标★的产品功能指标出现负偏离的，每项扣减0.5分，扣完为止。（非标★的产品，证明材料以技术偏离表为准） 注：防火墙（网络接入域）、态势感知平台（安全管理域）、无线电管理平台防护系统为核心产品，中标支付履约保证金后7个工作日内，甲方有权要求对本次投标产品进行性能压力测试及功能性验证，测试工作由甲方指定的第三方具有资质的机构完成，性能压力测试及功能性验证产生的所有费用均由中标单位支付，对于虚假应标者没收履约保证金做废标处理，并追究其相应法律责任；同时对推荐供应商按推荐顺序进行功能性验证测试，确定满足招标要求者为中标供应商。	40.00

评标步骤	序号	评审因素	评审标准	分值
	2	技术方案（满分4分）	评分规则根据投标人提供的技术方案进行评价。对项目背景、项目建设目标、项目建设任务及各项需求是否认识到位、理解充分，并提出有针对性的整体解决思路的程度进行评分： （1）情况了解最全面，详细描述了项目背景、项目现状、项目目标、项目需求，整体描述全面，整体部署架构合理，方案功能完善、提出针对性的解决思路，方案整体完整度和可行性高得4-3分。 （2）情况了解一般，简单描述了项目背景、项目现状、项目目标、项目需求，整体描述不够全面，方案功能基本满足、方案整体完整度和可行性一般得2-1分。 （3）未提供实施方案不得分。	4.00

评标步骤	序号	评审因素	评审标准	分值
	3	实施方案（满分3分）	评分标准：根据投标人提供的项目实施方案进行评价。项目实施内容、实施计划、具体实施措施、质量指标、时效指标、数量指标等内容进行评分： （1）实施方案中实施内容完整、实施计划可行性高、实施措施具体可靠，提出具体的质量指标、时效指标、数量指标等内容完善得3分； （2）实施方案中实施内容较完整、实施计划可行性较高、实施措施较为可靠，提出的质量指标、时效指标、数量指标等基本完善得2分； （3）实施方案中实施内容较完整、实施计划可行性较高、实施措施较为可靠，提出的质量指标、时效指标、数量指标等有缺陷得1分； （4）未提供实施方案不得分。	3.00

评标步骤	序号	评审因素	评审标准	分值
	4	服务方案（满分3分）	评分规则：根据投标人提供的售后服务方案进行评价，包括产品的培训、维护、维修的相关措施、响应时间、售后服务人员配置、处理故障的措施等内容进行评分： (1)、售后服务方案全面、深入，能够完全满足需求，并且在某些方面有显著的优势。执行计划周密，资源配置合理，管理到位，得3分。 (2)、售后服务方案基本符合要求，但在深度和广度上有所欠缺。执行计划和资源配置存在一定的问题，管理措施不够全面，得2分。 (3)、售后服务方案勉强达到基本要求，但存在较多的不足和缺陷。执行计划和资源配置不够合理，风险管理措施较为薄弱，得1分。 （4）未提供售后服务方案，未提供不得分。	3.00
政策性加分评审	1	节能环保加分	对投标产品属于“节能产品清单”或“环保产品清单”有效期内中的产品（强制采购产品除外），在招标采购评审工作过程中，给予适当加分，即在总得分基础上，每一项加0.3分；如投标产品同时属于“节能产品清单”和“环保产品清单”两个清单中产品的，每一项加0.5分，最高不得超过2分。	2.00

评标步骤	序号	评审因素	评审标准	分值
	2	少数民族加分	根据《中华人民共和国政府采购法》（中华人民共和国主席令第68号）、《中华人民共和国政府采购实施条例》（国务院第658号令）、贵州省财政厅文件（黔财采【2017】6号）的规定，对产品原产地在少数民族地区的投标主产品（不含附带产品）在总得分基础上加3分。注本项加分仅适用于货物采购项目；投标人应提供原产地证明材料如生产许可证、现场照片等 对原产地在少数民族自治区和享受少数民族自关品含附带产享受政策性加分在总得分基础上加3分。投标主产品按照不得低于本采购项目预算金额50%进行确定。①少数民族自治区内蒙古自治区、新疆维吾尔自治区、宁夏回族自广西壮族自治治区西藏自治区②享受少数民族自治待遇的省份青海省、云南省、贵州省。	3.00

评标步骤	序号	评审因素	评审标准	分值
报价评审	1	报价评审	(1)报价评审总报价 = 贵州省无线电管理信息系统网络安全建设项目 (2)报价评审得分 = （最低报价评审总报价 / 各投标人的报价评审总报价） * 30.00 备注：所报价均以扣除后的价格参与评审（若有）。 报价扣除说明: 小微型企业价格扣除率：10.00% 监狱、福利性企业视为：小微型企业 扣除后的金额报价=金额报价*（1-扣除率） 扣除后的下浮率报价=下浮率报价*（1+扣除率） 扣除后的折扣报价=折扣报价*（1-扣除率） 备注信息：投标人或产品若同时享有以上价格扣除情况的，仅对“投标报价分”进行一次价格扣除，并不作叠加扣除	30.00

第五章　采购需求

第一节 采购要求

一、项目概述

1、项目名称：贵州省无线电管理信息系统网络安全建设项目；

2、预算金额：270.00 万元，最高限价 264.00 万元。(（主中心节点）设备最高限价 215 万；备份中心节点最高限价 29 万元；集成费最高限价 20 万元）

3、项目概述:本期项目贵州省无线电管理信息系统网络安全建设项目将结合贵州省无线电监测站的实际情况，按照《网络安全等级保护基本要求》和《网络安全等级保护安全设计技术要求》等相关标准要求，以“一个中心、三重防护”为核心指导思想，针对贵州省无线电管理信息系统的业务应用、IT 基础设施及机房配套环境，进行安全技术体系、安全管理体系和安全运维体系构建。包括通过核心交换机、汇聚交换机、接入交换机、超融合服务器、超融合软件、出口边界防火墙、核心业务边界防火墙、病毒过滤网关/防毒墙、网络准入控制、WEB 应用防火墙、运维安全审计/堡垒机、数据库审计、全威胁检测系统和态势感知平台、日志审计、无线电管理平台防护系统、漏洞扫描、VPN 等网络安全设备构建安全技术体系，免费运维期内支撑贵州省无线电监测站从安全管理机构、安全管理人员、安全管理制度、安全建设管理、安全运维管理五个方面构建安全管理体系，免费运维期内支撑贵州省无线电监测站通过安全咨询服务、安全评估服务、安全加固服务、渗透测试服务、安全配置检查服务、应急响应服务、系统上线前检测服务等安全服务构建安全运维体系。

二、建设内容

涵盖贵州省无线电监测站主中心节点与备份中心节点的核心交换机、汇聚交换机、接入交换机、超融合服务器、超融合软件、出口边界防火墙、核心业务边界防火墙、病毒过滤网关/防毒墙、网络准入控制、WEB 应用防火墙、运维安全审计/堡垒机、数据库审计、全威胁检测系统和态势感知平台、日志审计、无线电管理平台防护系统、漏洞扫描、VPN 等货物的采购、安装、本机调试、联网调试等集成服务内容，包括二次深化设计、包装及运输、出厂检验、到货验收、分部

验收、单位验收、试运行、合同项目完成终验、质保、巡检、故障响应、维保、备品备件供应、技术培训、安全管理体系支撑服务、安全运行体系支撑服务等技术服务内容。

三、建设原则

1、标准符合性原则

构建贵州省无线电管理信息系统这样庞大的系统,必须坚持遵循相关的标准。本期目产品选型应遵循国家等级保护三级相关标准。

2、综合性、整体性原则

安全模块和设备的引入应该体现系统运行和管理的统一性。一个完整的系统的整体安全性取决于其中安全防范最薄弱的一个环节，必须提高整个系统的安全性以及系统中各个部分之间的严密的安全逻辑关联的强度，以保证组成系统的各个部分协调一致地运行。

3、易操作性原则

安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。

4、设备的先进性与成熟性

安全设备的选择，既要考虑其先进性，还要考虑其成熟性。先进意味着技术、性能方面的优越，而成熟性表示可靠与可用。

5、无缝接入

安全设备的安装、运行，应不改变网络原有的拓扑结构，对网络内的用户应是透明的，不可见的。同时，安全设备的运行应不会对网络传输造成通信“瓶颈”。

6、可管理性与扩展性

安全设备应易于管理，而且支持通过现有网络对网上的安全设备进行安全的统一管理、控制，能够在网上监控设备的运行状况，进行实时的安全审计。

四、建设依据

本次方案依据以下政策文件与相应技术规范进行设计。

1、政策文件

（1） 《中华人民共和国网络安全法》；
（2） 《中华人民共和国无线电管理条例》；
（3） 《“十四五”国家无线电管理和发展规划》；
（4） 《关于加强无线电监测工作的指导意见》（工信部无〔2019〕57 号）

；

（5） 《贵州省无线电管理“十四五”规划》。

2、技术规范文件

（1） 《信息系统灾难恢复规范》（GB/T 2098-2007）；

（2） 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）；

（3） 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

（4） 《网络安全等级保护设计技术要求》（GB/T 25070-2019）；

（5） 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）；

（6） 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

（7） 《省级无线电管理“十四五”规划技术设施建设实施方案》；

（8） 《省级无线电监测设施建设规范和技术要求（试行）》（国无办函〔2019〕3号）；

（9） 《省级无线电管理“一体化”平台建设规范及技术要求》（国无办函〔2019〕21号）；

（10） 建设单位提供的有关数据、资料及证明材料。

五、贵州省无线电管理信息系统网络安全建设项目建设方案

1.1 网络系统建设

1.1.1 建设思路

贵州省无线电管理信息系统网络架构设计在充分考虑业务连续性和数据安全性的基础上，采用双数据中心设计、光纤和 VPN 线路连接、虚拟化技术等先进的网络技术和设备，以实现网络的高速、安全和灵活性。

贵州省无线电管理信息系统网络基础设施涉及骨干网、接入网、局域网（含信息机房）、超融合扩容等方面的技术要求，需按照《省级无线电管理一体化平台建设规范及技术要求》开展配置。并利用现有云管中台，对一体化平台运行过程中各级信息化资源与设施的全链路分析与监控。

1.1.2 网络架构建设

贵州省无线电管理信息系统网络系统包括主中心节点和备份中心节点两个节点，主中心节点和备份中心节点之间通过光纤线路进行连接，以实现数据的实时备份和恢复，保证业务的连续性和数据的安全性。

主中心节点：包含网络接入域、核心交换域、安全运维域、核心业务数据区域、超融合

扩容集群、存储备份服务器集群区域、安全管理域、物联网卡接入区域、市州接入区域等网络区域。

备份中心节点：包含核心交换机、边界防火墙、日志审计、数据库审计、终端安全防护、数据存储集群等设备。

1.1.3IP 地址规划建设

1.1.3.1 省无线电管理信息系统中心节点 IP 地址规划设计

根据国家无线电监测中心分配，当前贵州省无线电管理信息系统专用网络 IP 地址段充足，结合未来 5 年贵州省无线电业务系统扩容情况考虑，对贵州省无线电监测指挥中心、各市州无线电管理机构及贵州省无线电管理信息系统中心节点（贵安新区）和贵州省无线电数据备份中心网络 IP 资源进行统一规划、合理划分，以满足未来贵州省无线电管理业务发展需求。

1.1.3.2 省无线电数据备份中心节点 IP 地址规划设计

对贵州省无线电数据备份中心，新增 3 个 C 类 IP 地址段做为备份网络设备、备份业务及备份业务预留 IP 地址。

1.1.4IPv6 设计

1.1.4.1IPv6 部署要求

2017 年 11 月 26 日，中共中央办公厅、国务院办公厅印发了《推进公共服务协议第六版（IPv6）规模部署行动计划》，明确了用 5 到 10 年时间，形成下一代公共服务自主技术体系和产业生态，建成全球最大规模的 IPv6 商业应用网络的目标。2018 年底商用网站前 50、省部级及其以上网站、域名服务商、超大型公共服务数据中心，TOP10 云服务商 50%云产品支持 IPv6。2020 年底商用网站前 100、地市级及其以上网站、域名服务商、超大型公共服务数据中心，TOP10 云服务商 100%云产品支持 IPv6。

1.1.4.2 双栈常用技术

双栈定义在 RFC4213 中，是指在终端设备和网络节点上既安装 IPv4 又安装 IPv6 的协议栈，从而实现分别与 IPv4 或 IPv6 节点间的信息互通。

双栈技术是 IPv4 向 IPv6 过渡的一种有效的技术，是 IPv4 向 IPv6 过渡的基础。网络中的节点同时支持 IPv4 和 IPv6 协议栈，源节点根据目的节点的不同选用不同的协议栈，而网络设备根据报文的协议类型选择不同的协议栈进行处理和转发。

网络对于 IPv6 应用系统的应用部署，可以采用新建 IPv6 应用试点的方式，建设 IPv4

服务器和 IPv6 服务器分开的结构，使用 IPv4 服务器对 IPv4 用户提供服务，使用 IPv6 服务器对 IPv6 用户服务；也可以采用 IPv4/IPv6 双栈服务器的结构，同时对 IPv4/IPv6 用户提供服务。

1.1.4.3IPv6 过渡设计

本项目中所有新增设备必须支持 IPv6，并进行 IPv6 过渡设计，整体设计方案采用 Underlay IPv4+Overlay IPv4/IPv6 双栈技术提供 Overlay 层面的 IPv4/IPv6 双栈能力；对于互访的其中一方为单栈 IPv4 网络，另外一方为双栈网络，仍通过 IPv4 协议栈完成互访，采用 Underlay IPv4+Overlay IPv4 进行业务互访。

1.1.5 超融合系统扩容设计

根据无线电监测中心数据承载资源需求，结合未来贵州省无线电业务系统扩容情况考虑，本次项目扩容两台物理服务器及 6 颗 CPU 超融合软件。

1.2 安全系统设计

1.2.1 设计思路

1.2.1.1 分区分域保护

用安全域方法论为主线来进行设计，从安全的角度来分析业务可能存在的安全风险。所谓安全域，就是具有相同业务要求和安全要求的 IT 系统要素的集合。这些 IT 系统要素包括：

网络区域

主机和系统

人和组织

物理环境

策略和流程

业务和使命

… …

因此，如果按照广义安全域来理解，不能将安全域的工作仅仅理解为在网络拓扑结构上的工作。

通过划分安全域的方法，将网络系统按照业务流程的不同层面划分为不同的安全域，各个安全域内部又可以根据业务元素对象划分为不同的安全子域。针对每个安全域或安全子域来标识其中的关键资产，分析所存在的安全隐患和面临的安全风险，然后给出相应的保护措

施；不同的安全子域之间和不同的安全域之间存在着数据流，这时候就需要考虑安全域边界的访问控制、身份验证和审计等安全策略的实施。

安全域划分以及基于安全域的整体安全工作，对贵州省无线电管理信息系统具有很大的意义和实际作用：

安全域划分基于网络和系统进行，是下一步安全建设的部署依据，可以指导系统的安全规划、设计、入网和验收工作；

可以更好的利用系统安全措施，发挥安全设备的利用率；

基于网络和系统进行安全检查和评估的基础，可以在运行维护阶段降低系统风险，提供检查审核依据；

安全域可以更好的控制网络安全风险，降低系统风险；

安全域的分割是出现问题时的预防，能够防止有害行为的渗透；

安全域边界是灾难发生时的抑制点，能够防止影响的扩散。

“同构性简化”的安全域划分方法，其基本思路是认为一个复杂的网络应当是由一些相通的网络结构元所组成，这些进行拼接、递归等方式构造出一个大的网络。同一区域内的资产实施统一的保护，如进出信息保护机制，访问控制，物理安全特性等。

1.2.1.2 全面纵深防御

本项目应以可信计算为基础，访问控制为核心，通过构建“一个中心支撑下的三重防护体系”的纵深防御体系来保障网站系统的安全。

“一个中心，三重防护”是指以安全管理中心为核心，构建安全计算环境、安全区域边界和安全通信网络，确保应用系统能够在安全管理中心的统一管控下运行，不会进入任何非预期状态，从而防止用户的非授权访问和越权访问，确保应用系统的安全。

安全管理中心是三重防护体系的控制中枢，是管理员的工作场所，管理员通过在安全管理中心制定安全策略，强制计算环境、区域边界执行策略，从而确保系统的运行环境是可信和安全。安全管理中心分成三个子系统：系统管理子系统、安全管理子系统、审计子系统，分别对应管理员的三个角色。系统管理子系统负责对安全保护环境中的计算节点、区域边界、通信网络实施集中管理和维护，包括用户身份管理、资源管理、应急处理等，为信息系统的安全提供基础保障。安全管理子系统是系统安全的控制中枢，主要实施标记管理、授权管理及策略管理等。安全管理子系统通过制定相应的系统安全策略，并且强制节点子系统、区域边界子系统、通信网络子系统执行，从而实现了对整个信息系统的集中管理，为重要信息的安全提供了有力保障。审计子系统是系统的监督中枢，系统审计员通过制定审计策略，强制

节点子系统、区域边界子系统、通信网络子系统、安全管理子系统、系统管理子系统执行，从而实现对整个信息系统的行为审计，确保用户无法抵赖违背系统安全策略的行为，同时为应急处理提供依据。

计算环境是应用系统的运行环境，包括应用系统正常运行所必须的终端、服务器、网络设备等，计算环境安全是应用系统安全的根本；计算环境由节点子系统和应用防护子系统构成。节点子系统通过在操作系统核心层、系统层设置以强制访问控制为主体的系统安全机制，形成了一个严密牢固的防护层，通过对用户行为的控制，可以有效防止非授权用户访问和授权用户越权访问，确保信息和信息系统的机密性和完整性安全，从而为应用系统的正常运行和免遭恶意破坏提供支撑和保障。应用防护子系统承接了安全操作系统和上层应用系统，直接支撑着应用系统的安全。应用防护子系统通过对应用服务的封装，不仅实现了对应用系统访问控制，而且增强了应用系统运行环境的隔离性，使得应用系统不受非授权进程的恶意干扰，保护了信息的保密性和完整性。

区域边界是应用系统运行环境的边界，是应用系统和外界交互的必经渠道，通过区域边界的安全控制，可以对进入和流出应用环境的信息流进行安全检查，既可以保证应用系统中的敏感信息不会泄漏出去，同时也可以防止应用系统遭受外界的恶意攻击和破坏。

通信网络是不同应用系统之间进行信息交互的通道，安全的通信网络设备能够保证应用系统之间交互信息的机密性和完整性。三重防护体系为应用系统构建了一个严密的立体防护网，既能够防止应用环境之内的用户对系统安全进行破坏，又能够防止内外部用户对系统安全的破坏，即能够做到“防内为主，内外兼防”，可以有效保护高等级应用系统的安全。

1.2.1.3 动态综合防护

根据中办发【2003】27 号文件，“坚持积极防御、综合防范的方针，全面提高信息安全防护能力”是国家信息保障工作的总体要求之一。“积极防御、综合防范”是指导等级保护整体保障的战略方针。

安全保障不是单个环节，单一层面上问题的解决，必须是全方位地、多层次地从技术、管理等方面进行全面的安全设计和建设，“积极防御、综合防范”战略要求信息系统整体保障综合采用覆盖安全保障各个环节的防护、检测、响应和恢复等多种安全措施和手段，对系统进行动态的、综合的防护，在攻击者成功地破坏了某个保护措施的情况下，其他保护措施仍然能够有效地对系统进行保护，以抵御不断出现的安全威胁与风险，保证系统长期稳定可靠的运行。

1.2.2 安全架构设计

贵州省无线电管理信息系统安全架构分为安全管理体系、安全技术体系、安全运维体系。三个体系有机结合，相互支撑。

总体安全保护架构设计以等级保护“一个中心、三重防护”为核心指导思想，构建集防护、检测、响应、恢复于一体的全面的安全保障体系。以全面贯彻落实等级保护制度为核心，打造科学实用的网络安全防护能力、安全风险监测能力、应急响应能力和灾难恢复能力，从安全技术、安全管理、安全运维三个维度构建安全防护体系，切实保障网络安全总体防护水平。

安全管理体系：是为保障网络安全而采取的一系列管理措施的总和，内容主要包括建立健全网络安全组织体系、网络安全策略体系、风险管理安全策略等。

安全技术体系：是为保障网络安全而采取的一系列技术措施的总和，内容主要包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心以及核心产品自主可控安全等。

安全运维体系：是为保障管理措施和技术措施有效实现网络安全而采取的一系列活动的总和，内容主要包括日常运维管理机制、安全评估、安全加固、安全巡检、应急响应、安全通告、安全培训、上线检测以及安全服务等。

1.2.3 等级保护定级分析

基于 GA/T1389-2017《网络安全等级保护定级指南》之要求，对等级保护定级主体进行了扩展，贵州省无线电监测站所辖范围内的基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等，都将根据其在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，确定其定级。

1.2.4 安全技术体系设计

等级保护方案设计必须架构在科学的安全体系和安全框架之上。安全框架是安全方案设计和分析的基础。为了系统地描述和分析安全问题，根据贵州省无线电管理信息系统的业务要求和国家对网络等级保护的有关规定，本节将从层次结构的角度展开，详细分析贵州省无线电管理信息系统各个层次可能存在的安全漏洞和安全风险，并提出解决方案。

我们从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等几个层面提出所采用的安全技术和措施。

1.2.4.1 安全物理环境设计

本项目的安全物理环境设计由贵州省无线电管理信息机房设施建设项目考虑，安全物理

环境主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。具体包括：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。

1.2.4.2 安全通信网络设计

安全通信网络重点关注的安全问题：一是网络架构的安全，包括网络安全区域的合理划分，重要网络区域部署和防护；主干网络的可用性，包括通信链路和节点设备的冗余、网络带宽的合理分配；网络通信中数据完整性和保密性的防护等。还有就是安全通信网络设备的可信验证。因此，在安全通信网络层面，需要采用的安全技术手段包括：

1.2.4.2.1 网络架构安全

贵州省无线电管理信息系统网络目前没有进行安全区域的划分，无法基于安全域进行访问控制和入侵防范。按照方便管理和控制的原则，对网络划分不同的安全区域，并为各安全区域分配相应的地址和设置默认路由。在安全域划分基础上可方便地进行网络访问控制、网络资源（带宽、处理能力）管控等安全控制，并对不同安全域边界的保护策略进行针对性设计。

1.2.4.2.1.1 安全域划分

根据《省级无线电管理一体化平台建设规范及技术要求》及《无线电管理一体化平台集成规范 第 4 部分：应用安全》，从数据安全、网络安全、边缘安全等开展防护，并建立安全管理中台，总体分为接入域、业务域、安全管理域和安全运维域四个域进行安全防护管理。

1、接入域：

（1）网络接入域：上联国家无线电监测中心区域分中心、下联各地市，以及与省本级移动站进行数据交互接入的网络区域。

（2）物联网卡接入域：包含物联网卡接入系统（众包、网格化等系统）等系统的 VPN 接入。

（3）DMZ 接入域：对外提供数据的 DMZ 接入

2、业务域：

（1）网闸接入域：执法系统等数据安全交换接入。

（2）核心业务数据区域：承载业务应用、数据存储等的服务器和一体化平台。

（3）核心交换域：核心网络数据转发、交换。

3、安全管理域：集中部署各类安全设备的区域。

4、安全运维域：运维人员进行日常运维的区域。

地市网络中，上联至贵州省监测站网络的区域定义为接入域。

根据实际需求，配置防火墙（网络接入域）、防火墙（核心业务域）、病毒过滤网关/防毒墙（网络接入域）、网络准入控制（安全管理域）、Web 应用防护（核心业务域）、运维安全审计（安全管理域）、数据库审计（核心业务域）、全威胁检测系统（核心交换域）、日志审计（安全管理域）、态势感知平台（安全管理域）、无线电管理平台防护系统（安全管理域）、漏扫（安全管理域）、VPN 网关（网络接入域）。

1.2.4.2.1.2 区域边界隔离（VLAN/下一代防火墙）

在安全域划分的基础上，利用路由交换设备自身的能力，按照用户实际需求，对内部网络不同安全域划分不同逻辑子网（VLAN），并在 VLAN 之间定义访问控制规则（ACL），实现网络内部不同安全域之间的基本隔离。

在此基础上，建议在贵州省无线电管理信息系统的接入链路与核心交换机之间、核心业务数据区域接入交换机与核心交换机之间分别串联部署下一代防火墙，实现内外网安全隔离和内部不同网络区域之间的安全隔离。通过设置相应的网络地址转换策略和端口控制策略，避免将重要网络区域直接其他网络区域直接连通。

1.2.4.2.1.3 高可用性设计

单线路、单设备的结构很容易发生单点故障导致业务中断，因此对于提供关键业务服务的信息系统，应用访问路径上的任何一条通信链路、任何一台网关设备和交换设备，都应当采用可靠的冗余备份机制，以最大化保障数据访问的可用性和业务的连续性。

建议在贵州省无线电管理信息系统中，除了接入链路应采用多运营商链路互备、关键业务系统应采用多服务器互备外，对于局域网骨干核心链路及相关的网络路由交换设备、安全网关设备等均采用冗余热备的部署方式，以提升网络系统的整体容错能力，防止出现单点故障。

1.2.4.2.2 通信传输安全（VPN）

对于贵州省无线电管理信息系统注册用户及移动办公、远程运维人员通过边界登录到网站系统进行的业务交互操作或远程管理操作，需要采用 IPSEC 或 SSL VPN 技术保证重要、敏感信息在网络传输过程中完整性和保密性。

安全接入管理

通过结合使用数字证书与专用 VPN 客户端软件，实现接入身份以及设备的准确识别、对接入终端的安全管理，保证系统接入过程的安全可靠。

传输过程安全管理

借助IPSEC或SSL VPN技术的隧道加密技术实现网络通信过程及数据传输过程的安全，并且可根据不同人员的角色确认应用的访问权限，实现随时随地，按需接入及受限访问，最大程序保证传输过程安全。

接入及传输过程管理

通过接入管理端对接入人员及接入设备进行统一管理，可实现人员的角色及权限的统一管理，实现不同角色访问不同的访问咨询。针对接入设备的安全性问题，通过对设备进行合规性检查，确保设备接入后不会给网络带来风险。通过对接入过程进行安全审计，实时掌握接入及传输过程的状态并对网络接入及传输行为进行审计。

1.2.4.3 安全区域边界设计

安全区域边界是对内部应用系统计算环境进行安全防护和防止敏感信息泄露的必经渠道；通过区域边界的安全控制，可以对进入和流出应用环境的信息流进行安全检查，既可以保证应用系统中的敏感信息不会泄漏出去，同时也可以防止应用系统遭受外界的恶意攻击和破坏。

1.2.4.3.1 边界防护

在网络边界需要部署防火墙对边界进行安全访问控制及安全检测，保证跨越边界的访问和数据流是通过边界防护设备提供的受控接口进行通信的。另外对于用户通过其他手段接入监测业务（如无线网卡、双网卡、modem拨号上网），或使用非授权设备接入内网，这些边界防御则形同虚设。因此，必须在全网中对网络的接入和外联进行连接状态的监控，准确定位并能及时报警和阻断。

1.2.4.3.1.1 边界通信控制（下一代防火墙）

建议在贵州省无线电管理信息系统的边界接入链路与核心交换机之间、核心业务数据区域接入交换机与核心交换机之间分别串联部署下一代防火墙，确保所有跨越边界的访问和所有流入、流出的数据均通过其受控接口进行通信、接受安全检查和处理。

1.2.4.3.1.2 网络准入控制

通过在贵州省无线电管理信息系统内部办公区域部署专业的网络准入控制设备来进行严格的网络接入监控。要求所有内网终端在准入网关上进行注册，并结合交换机开启的802.1X端口认证功能，确保只有认证通过的机器才能够接入网络，拒绝未经授权的机器接入内网或将其隔离到一个单独的网络区域进行受限的网络访问。或者如果终端安全状况检查（如防病毒软件、安全补丁等）没有达标，则交换机可以根据准入网关的指令，将其隔离到一个修复区，修复安全状况，一旦安全修复完成，准入网关会通知交换机将该终端从修复区

切换到正常工作的 VLAN 之中。在接入终端安全状况检查通过后，准入网关将根据用户所属角色或所具备的权限来动态分配其工作 VLAN。准入网关也支持对私自修改 IP 地址的行为进行实时监视和阻断，防止内网 IP 地址滥用影响正常网络通信。

网络准入控制系统提供以下功能：

网络准入身份认证：基于 802.1X 方式实现准入，通过对支持此协议的交换机进行管理，利用交换机 LAN 架构的物理特性，实现 LAN 端口的设备认证。只有安装客户端且具有合法账号的终端计算机才能通过认证。

合规性健康检查：终端计算机在入网身份认证通过后，进入终端安全合规检测环节，并通过评分制的形式对终端的健康状况做最后的评估。只有通过合规检测的，才能顺利通过入网认证管理，否则隔离处理，即入网必合规。可以参考的合规检测项目：系统时间、系统运行时长、Guest 用户、Windows 文件共享、Windows 防火墙、必须运行的进程、必须运行的服务、必须安装的软件、禁止安装的软件、是否安装防病毒软件及病毒库是否为最新版本、是否安装最新的系统和软件补丁等。

接入管理：结合健康检查结果，通过服务器和网络设备以及终端 PC 联动来决定，包括：拒绝终端/用户接入；允许终端/用户接入；隔离终端/用户（终端 IP 管理，VLAN 隔离）；限制终端/用户访问权限。

隔离修复：在隔离或者限制接入的情况下，还可以通过修复向导来恢复正常的网络访问权限。修复向导提供安全修复页面，客户端根据修复向导进行安全修复。

终端软硬件资产管理：对终端的软硬件资产信息进行采集，并对资产变化进行监测、报警，全面统计资产信息。

1.2.4.3.1.3 双向网闸数据安全交换（利旧）

建议在贵州省无线电监测站执法系统、一网通办等重要系统与核心交换机之间部署双向网闸系统，既实现网络安全隔离又实现交互数据的安全交换。

安全 Web 浏览：支持 http 和 https 协议，提供网页访问和控制功能。屏蔽外网 Web 站点上有害内容的侵扰，保护内网 Web 应用不受外来访问的恶意攻击

FTP 文件交换：保护内网 FTP 服务器不受攻击。除受控通道的基本安全支持外，FTP 协议还可对使用 FTP 通道传输的内容进行过滤，包括病毒等恶意代码的查杀。

数据库访问：在内外网隔离的环境下，实现内外网之间的数据库访问。

文件同步：实现两个网络间的文件实时交换。

数据库同步：保证不同安全等级网络中的数据库中数据的实时同步更新。

1.2.4.3.2 访问控制

由于贵州省无线电管理信息系统是面向监测业务提供开放服务，很容易受到来自内外部网络的非法访问和恶意攻击。借助基于深度包检测技术的网络访问控制机制，可对进出网络边界的通信报文、应用会话和数据内容进行检查，拦截非授权访问行为和非法数据通信。

1.2.4.3.2.1 协议级访问控制（下一代防火墙）

在贵州省无线电管理信息系统的边界接入链路与核心交换机之间、核心业务数据区域接入交换机与核心交换机之间分别串联部署下一代防火墙，确保所有跨越边界的访问和所有流入、流出的数据均通过其受控接口进行通信、接受安全检查和处理。根据业务需要制定防火墙的访问控制策略，在缺省拒绝所有通信的基础上，仅允许业务所需的访问连接和数据通信。

下一代防火墙具备以下基本功能：

安全隔离：防火墙串接部署在核心交换机与边界接入链路、各网络区域接入交换机之间，实现内外网安全隔离和内部不同网络区域之间的安全隔离。

网络访问控制：防火墙工作在网络出口及不同网络区域之间，对内外网络之间及内部各个网络区域之间流转的数据进行深度分析，依据数据包的源地址、目的地址、通信协议、端口、流量、用户、通信时间等信息进行判断，确定是否存在非法或违规的操作，对不符合允许转发策略的流量进行阻断，从而有效保障网络安全。

会话监控：在防火墙配置会话监控策略，当会话处于非活跃一定时间或会话结束后，防火墙自动将会话丢弃，访问来源必须重新建立会话才能继续访问资源。

防范带宽滥用：可基于应用内容而非协议端口识别包括传统协议、P2P 下载、股票交易、即时通讯、流媒体、网络游戏、网络视频等常见网络应用，并能够详细统计每一种应用的流量、连接数和累积传输字节数，判断网络中的各种带宽滥用行为，继而采取包括阻断、限制连接数、限制流量等各种控制手段对网络应用访问流量进行精细化管理，确保关键应用或重要用户的带宽使用，确保网络业务通畅，满足业务高峰期带宽需要。

1.2.4.3.3 入侵防范（下一代防火墙开通入侵防御功能模块）

针对边界上常见的漏洞利用攻击、SQL 注入攻击、XSS、缓冲区溢出、DOS/DDOS 攻击等恶意破坏方式，综合采用入侵检测和防御、异常流量管理与抗拒绝服务攻击、未知威胁防御等安全机制，阻断恶意的网络数据包，有效保证网站服务器正常提供服务。

1.2.4.3.3.1 网络入侵防御（下一代防火墙开通入侵防御功能模块）

建议在贵州省无线电管理信息系统的边界接入边界防火墙上启用入侵防御功能，实时发

现和阻止从内外部网络发起的网络攻击行为；同时可在内部计算区、安全管理区边界防火墙上均启用入侵防御功能，阻止来自其它网络区域的攻击流量。

下一代防火墙可实现以下入侵防御功能：

防范网络攻击：综合采用模式匹配、协议分析、统计分析、流量异常检测、会话关联分析以及防逃逸等技术手段准确识别入侵攻击行为，为用户提供 2~7 层深度入侵检测能力。支持发现并阻断包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等在内的各种网络恶意攻击。

防范拒绝服务攻击：通过构建统计性攻击模型和异常包攻击模型，可以全面防御 SYN flood、ICMP flood、UDP flood、ARP Flood、DNS Flood、DHCP flood、Winnuke、TcpScan 以及 CC 等常见 DOS/DDOS 攻击行为。

防范带宽滥用行为：可根据数据内容而非端口智能识别包括传统协议、P2P 下载、股票交易、即时通讯、流媒体、网络游戏、网络视频等常见网络应用，并能够详细统计每一种应用的流量、连接数和累积传输字节数，判断网络中的各种带宽滥用行为，继而采取包括阻断、限制连接数、限制流量等各种控制手段，确保网络业务通畅。

1.2.4.3.3.2 未知威胁防御（全威胁检测系统）

在贵州省无线电管理信息系统局域网核心交换机上部署全流量监测设备，提供集合恶意程序检测、DDoS 检测、攻击检测、僵尸主机检测、URL 检测、威胁情报、IP 黑白名单检测等多种检测引擎，能够对网络中的异常流量、异常行为、异常信息、异常文件传输监测。通过多维的检测模式，精准有效识别网络中漏洞攻击、Web 攻击、木马蠕虫、僵尸主机、恶意文件等威胁。同时，能够探测网络中潜在的高级可持续攻击威胁。主要功能如下：

攻击检测

支持对扫描攻击、缓冲区溢出攻击、拒绝服务攻击、漏洞扫描攻击、蠕虫病毒攻击、非授权访问攻击、后门木马攻击、文件漏洞攻击等常见攻击行为检测。

具有防逃逸检测能力，做到从根源上检测逃逸行为攻击。支持对 IP 分片逃逸行为、TCP 流重组逃逸行为、协议端口重定向逃逸行为、URL 变形逃逸行为等多种逃逸行为攻击识别。

具备 DNS 投毒检测能力。

支持从源目 IP、MAC 等维度分析 ARP 请求、响应的合法性。

账号安全检测

根据密码字典和口令强度双重模式实现对弱口令的攻击检测，设备检测到密码符合弱口令字典或者密码符合配置的密码强度，则会判断为弱口令。可支持对邮件协议、文件协议、

远程连接协议、数据库协议、web 应用多种协议识别检测，有效应对弱口令攻击行为。

判断在配置的周期时间内登录失败的次数超过了配置的检测次数，需要超过检测次数，登录成功检测次数等多种检测方式。支持对邮件协议、文件协议、远程连接协议、数据库协议、web 应用多种协议识别检测，有效应对暴力破解攻击行为。

僵尸木马蠕虫病毒检测

对网络中协议异常、访问异常、连接异常的主机提取通信行为特征，采用木马特征库匹配的方式检测网络中木马、蠕虫的活动行为，从而识别定位网络中的僵尸主机。支持对僵尸网络行为、木马控制行为、蠕虫活动行为、勒索病毒行为、移动端木马控制行为等多种僵尸主机行为检测。对被检测到的僵尸主机异常行为，支持对异常行为报文取证、事件记录，事件记录包括攻击源信息、事件应用协议、事件描述等信息。

DDoS 检测

支持对 IP 扫描攻击、端口扫描攻击等多种扫描类的 DDoS 攻击检测。支持对 ICMP FLOOD、TCP FLOOD、UDP FLOOD、SYN ACK FLOOD、FIN FLOOD、RST FLOOD、DNS FLOOD、HTTP FLOOD、HTTPS FLOOD 等多种 FLOOD 攻击行为检测。

恶意程序检测

对网络中使用 HTTP、FTP、SMTP、POP3、SMB、DNS、NFS、IMAP 等非加密协议以及 HTTPS、FTPS、SMTPS、IMAPS 等加密协议传输的文件，采用特征检测、TAI 智慧引擎、虚拟沙箱、第三方联动等多种技术手段检测是否存在恶意程序。

APT 检测

依靠威胁情报库中多种 APT 威胁情报信息对 APT 进行检测，包含 APT 攻击涉及的恶意 IP、恶意域名、恶意 URL、恶意文件等情报。通过对 APT 威胁情报的感知，可在 APT 攻击的早期阶段，提前防控 APT 风险。

依靠智慧引擎+虚拟沙箱检测方式，对未知恶意代码检测，从而检测出未知 APT 事件。

通过僵尸主机行为库检测异常主机行为的方式，识别网络中活跃的 APT 组织，对 APT 攻击组织的异常行为监测。

WEB 安全检测

支持对 SQL 注入攻击、跨站攻击、浏览器劫持攻击、URL 跳转攻击、目录遍历攻击、WEB 缓冲区溢出攻击、WEB 漏洞攻击、WEB 越权攻击、WEB 远程代码执行攻击、WEB 扫描攻击、Webshell 上传攻击、文件上传、爬虫等多种类型的 WEB 攻击检测。

虚拟沙箱

虚拟沙箱中的系统环境中具有文件系统、注册表系统、窗口系统等多种操作系统核心机制，达到高度仿真效果，具有跨平台特性。执行引擎具有虚拟化执行引擎和动态翻译执行引擎两种，两种执行引擎的结合既能保证对文件的执行效率达到与真实机相当，又能实现对目标代码的细粒度控制。

威胁情报

威胁情报库是从海量的威胁情报中提取出 800 万+高可信威胁，检测威胁类型多维，检测速度快。产品的威胁情报功能在满足精准、高效的同时，也保持高频率更新，及时更新热点威胁情报信息。

异常流量检测

对服务器外联行为进行监控，检测服务器是否会主动和外部进行通信（可能中毒），针对异常的通信行为会进行告警并上报管理员进行进一步的处理，系统支持服务器非法外面检测并支持外联自学习。

通过 AI 深度学习技术中的循环神经网络（Recurrent Neural Network, RNN），对海量恶意域名样本充分训练生成检测模型来识别网络中伪随机域名，解决 DGA 域名算法逆向破解难题，实现对隐秘性高的 DGA 恶意域名进行深入检测。RNN 具有自动提取样本特征的能力，可挖掘其内在的字符分布统计特征，将传统方法的分类精度大幅度提升，实现检测率高，误报率，漏报率低。

针对失陷主机异常外联通信行为进行非法外联监测，做到从内到外的威胁监测能力。对通信协议采用智能分析的手段，能够有效识别僵尸主机使用“私有”协议建立的隐秘通信通道。采用异常行为检测+智慧引擎检测多种手段，对 DNS 隧道、ICMP 隧道、HTTP 隧道的异常通信监测，排查失陷主机异常请求，通过发现主机异常通信行为来深入检测隐蔽隧道。

加密流量检测

通过导入证书+无证书检测相结合的方式，直接对加密流量进行解密处理，实现对加密流量元数据的深度提取，检测恶意威胁信息。设备通过智慧引擎检测、异常握手检测、非法证书检测、内网流量检测等多种方式发现恶意程序的加密通信，实现无证书检测加密通信的效果。由天融信安全研究团队通过对恶意程序行为进行深入分析，提取出恶意程序加密通信的指纹特征，从而生成指纹特征库。

溯源取证

支持对入侵攻击、僵尸网络、恶意程序等威胁事件进行取证记录，支持流量报文取证和样本文件取证。具备全流量取证能力，能将恶意事件的事前、事中、事后流量全部抓取存留。

系统将安全事件元数据信息和取证文件关联，用户通过对威胁基本元数据检索的方式即可获取全面的威胁信息，友好支撑用户对威胁的深入溯源分析。

URL 检测

地址库种类全面、详细，包括搜索引擎、社交网络、网上购物、求职招聘、休闲娱乐、财经、恶意网站、非法及不良、成人内容、网络安全、下载网站等地址，通过对网络中 URL 的识别，精准有效发现用户对非法网站的访问动作，有利于对威胁、恶意风险的控制。

元数据提取

支持对 TCP/UDP 流量、ICMP 流量、HTTP 流量、邮件流量、FTP 流量、DNS 流量、NFS 流量、SMB 流量、SSL 流量、LDAP 流量、RDP 流量等多种非加密流量以及 HTTPS 流量、加密邮件流量、FTPS 流量等多种加密流量深度提取元数据信息。提取的元数据，除基本的五元组信息外，还具有多种类型的内容层信息，如邮件元数据、文件元数据、URL 访问元数据等。

流量分析

对所有网络数据流通过流量解析、协议还原、会话关联等方式实现全面的流量分析。支持按接口对报文流入流出速率实时监控，每分钟对接收的报文按传输层协议、网络层协议、报文字节大小等多维度进行统计分析。对各接口的流量趋势按天、周、月图形化记录。

资产识别

支持识别网络中的资产信息，具备资产识别能力，帮助用户全面掌握当前网络资产情况。主动识别是从镜像采集的网络流量中主动解析存在的资产信息，识别效率高。被动扫描是对指定网络中存在的活跃资产信息全面深度扫描，扫描结果更全面。

资产信息记录资产 IP、MAC、操作系统、资产类型、分组、具有的应用服务列表等详细信息。

1.2.4.3.4 恶意代码和垃圾邮件防范

1.2.4.3.4.1 病毒过滤网关（下一代防火墙开通防病毒过滤功能模块）

在贵州省无线电管理信息系统的边界出口边界部署病毒过滤网关，在核心业务数据区域边界下一代防火墙上开启病毒过滤网关功能，对进出的网络数据流进行病毒、恶意代码扫描和和过滤处理，并提供病毒代码库的自动或手动升级，彻底阻断内外部网络的病毒、蠕虫、木马及各种恶意代码向网络内部传播。

病毒过滤网关与部署在终端、服务器上的防病毒软件相配合，从而形成覆盖全面，分层防护的多级病毒过滤系统。作为边界防护设备，病毒过滤网关提供以下的安全功能：

网络病毒过滤：对 SMTP、POP3、IMAP、HTTP 和 FTP 等应用协议进行病毒扫描和过滤，通过恶意代码特征过滤，对病毒、木马、蠕虫以及移动代码进行过滤、清除和隔离，有效地防止可能的病毒威胁，将病毒阻断在进入网络之前。

内容过滤：对数据内容进行检查，可以采用关键字过滤，URL 过滤等方式来阻止非法数据进入网络。支持通过文件内容识别文件类型，有效的阻断非法类型的文件进入网络。

恶意代码防护：支持对移动代码如 Vbscript、JAVA script、ActiveX、Applet 的过滤，能够防范利用上述代码编写的恶意脚本进入网络。

蠕虫防范：可以实时检测到日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止信息网络因遭受蠕虫攻击而陷于瘫痪。

病毒库升级：病毒过滤网关支持自动和手动两种升级方式，在自动方式下，系统可自动到边界上的厂家网站搜索最新的病毒库和病毒引擎，进行及时的升级。

日志记录：提供完整的病毒日志、访问日志和系统日志等记录，并支持发送给集中的日志审计服务器。

1.2.4.3.5 安全审计

安全审计通过收集并分析系统日志等数据，从而发现违反安全策略的行为。与入侵检测相比，安全审计主要侧重于事后分析，即当发生安全事故或者发生违反安全策略的行为之后，通过检查、分析、比较审计系统收集的数据，从中发现违反安全策略行为。

1.2.4.3.5.1 网络安全审计（数据库审计）

为了对特定用户的网络访问行为和内容进行更细粒度的审计追踪，可在贵州省无线电管理信息系统内部网络中部署专门的网络审计系统。将网络审计设备连接在核心交换机上，通过旁路侦听的方式进行数据采集，能够分析网络中的数据包、流量信息，通过对相关协议进行分析，对网络通信行为和内容进行记录和统计，帮助发现网络中的异常流量和违规行为。网络审计的重点对象是内网用户终端的网络访问行为，支持多种网络应用协议的监控、还原和审计，例如对通过 HTTP、FTP、SMTP 等方式访问业务系统的用户登录、用户登录 IP 地址、访问时间、访问内容等进行监控和审计。

网络审计系统具有即时的网络数据采集能力、强大的审计分析功能以及智能的信息处理能力，主要功能如下：

网络行为和传输内容实时监测和审计取证：对服务器区域的应用访问进行网络访问行为的监控和网络传输内容的审计，可根据管理人员的需求进行审计策略的设置（如本单位职工是否在工作时间做与工作无关的事情、是否通过网络泄漏了本单位的机密信息等等），实

现网络行为后期取证，对网络潜在威胁者予以威慑。

HTTP 监控：截获、记录、回放、归档被监测网段中所有用户浏览内容，包括各种文件，如 HTML 文件、图像文件、文本文件等。

内容监控：对特定应用系统进行监控；对指定端口，指定 IP 地址或 IP 段进行监控；根据设定的关键词或关键字组合自动对网页内容查询、分析、统计、检查。

电子邮件监控：完全截获、记录、回放、归档被监测网络中所有用户收发的电子邮件，内容包括：收件人和发件人各自的邮件地址、收件人和发件人各自的 IP 地址、电子邮件的主题、电子邮件的内容、电子邮件附件的完全还原，并可将附件导出、对压缩的附件进行最多十四层的解压。

远程登陆监控：记录、查询访问服务上 TELNET 用户名、口令字；记录和回放用户在服务器上的操作过程；对指定端口，指定 IP 或 IP 地址段进行监控；根据设定的关键词或关键字组合自动对传输的内容查询、分析、统计，对符合条件的相关内容形成证据文件，提供强有力的监控证据文件。设定的条件包括指定时间、指定 IP 地址或 IP 段、协议、用户名；最后按照用户指定的条件，生成报表。

网上邻居监控：对 NETBIOS 和 SMB 协议进行解码、分析和还原；记录和报告用户访问过的“网上邻居”上的其他主机 IP 和名称；记录、报告用户访问过的“网上邻居”中的各种资源，包括文件、目录、打印机等；对指定端口，指定 IP 或 IP 地址段进行监控；最后按照用户指定条件，生成报表。

审计数据保护：审计的内容采取单独的服务器和单独的数据库进行存放，并在审计数据库边界采取足够的安全防护措施，要保证除安全管理人员以外，任何人均无法单独中断审计进程，无法删除、修改或覆盖审计记录。

1.2.4.3.5.2 日志审计

在贵州省无线电管理信息系统网络中所有网络设备和新增的边界安全设备上均开启完整的日志记录功能，对重要的用户行为和重要安全事件进行审计，并将审计记录实时发送给集中的日志服务器，便于长期存储保护和分析使用。

1.2.4.4 安全计算环境设计

计算环境是应用系统的运行环境，包括应用系统正常运行所必须的主机（终端、服务器、网络设备等）、应用系统、数据、存储与备份等，计算环境安全是应用系统安全的根本。

计算环境的安全设计如下：

1.2.4.4.1 主机安全

主机系统安全是包括服务器、终端/工作站等在内的计算机设备、网络设备自身等在操作系统及数据库系统层面的安全。终端/工作站是带外设的台式机与笔记本计算机，服务器则包括应用程序、网络、web、文件与通信等服务器，网络设备则包括路由器、交换机、防火墙等。主机系统是构成信息系统的主要部分，其上承载着各种应用。因此，主机系统安全是保护信息系统安全的中坚力量。

主机系统安全可从：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证等方面进行安全建设。

1.2.4.4.1.1 运维安全管控和审计（运维安全审计）

建议在贵州省无线电管理信息系统网络的安全管理区部署一套运维审计系统（堡垒主机），在系统运维人员和信息系统（网络、主机、数据库、应用等）之间搭建一个唯一的入口和统一的交互的界面，针对信息系统中关键软硬件设备运维的行为进行管控及审计。通过将各设备、应用系统的管理接口，通过强制策略路由的方式，转发至堡垒主机，从而完成反向代理的部署模式，实现对管理用户的身份鉴别。通过“数字证书”认证方式作为“用户名+口令”验证身份的有效补充和增强，实现等级保护三级要求的双因素身份认证。

运维安全审计主机主要实现功能包括：

单点登录：提供基于 B/S 的单点登录系统，用户通过一次登录系统后，就可以无需认证的访问包括被授权的多种基于 B/S 的应用系统，使用户无需记忆多种登录用户 ID 和口令。单点登录可以实现与用户授权管理的无缝链接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。

集中账户管理：支持对所有服务器、网络设备登录帐号的集中管理，是集中授权、认证和审计的基础，降低了管理大量用户帐号的难度和工作量。同时，还能够制定统一的、标准的用户帐号安全策略。集中帐号管理可以实现将帐号与具体的自然人相关联，从而实现针对自然人的行为审计。

统一身份认证：为用户提供统一的认证接口。采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性，同时又避免了直接在业务服务器上安装认证代理软件所带来的额外开销。集中身份认证提供静态密码、数字证书、一次性口令和生物特征等多种认证方式，而且提供接口，可以方便地与第三方认证服务对接。建议采用基于静态密码+数字证书的双因素认证方式。

统一资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户

通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。授权的对象包括用户、用户角色、资源和用户行为。系统不但能够授权用户可以通过什么角色访问资源这样基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及在什么时间进行操作等的细粒度授权。

细粒度访问控制：提供细粒度的访问控制，最大限度保护用户资源的安全。细粒度的命令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，来限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。访问控制策略是保护系统安全性的重要环节，制定良好的访问策略能够更好的提高系统的安全性。

操作审计：操作审计管理主要审计操作人员的帐号使用（登录、资源访问）情况、资源使用情况等。在各服务器主机、网络设备的访问日志记录都采用统一的帐号、资源进行标识后，操作审计能更好地对帐号的完整使用过程进行追踪。为了对字符终端、图形终端操作行为进行审计和监控，堡垒主机对各种字符终端和图形终端使用的协议进行代理，实现多平台的操作支持和审计，例如 Telnet、SSH、FTP、Windows 平台的 RDP 远程桌面协议，Linux/Unix 平台的 X Window 图形终端访问协议等。

1.2.4.4.1.2 日志审计

在贵州省无线电管理信息系统的所有服务器操作系统、应用系统和新增的各种安全系统均开启完整的日志记录功能，对重要的用户行为和重要安全事件进行审计，并将审计记录实时发送给集中的日志服务器，便于长期存储保护和分析使用。

1.2.4.4.1.3 网络漏洞扫描

网络漏洞扫描系统基于网络，通过远程检测目标系统 TCP/IP 不同端口所提供的服务，分析目标给予的应答，以搜集目标系统上的各种信息，然后与系统内置的漏洞库进行匹配，如果满足匹配条件，则认为安全弱点存在。

建议在贵州省无线电管理信息系统网络中部署一套网络漏洞扫描系统，由专门的管理员负责，可以连接在核心交换机上，或根据需要连接到各网络区域中，以本地扫描或远程扫描的方式，对各台重要的网络设备、主机系统及相应的操作系统、应用系统等进行全面的漏洞扫描和安全评估。通过从不同角度对网络进行扫描，可以发现网络结构和配置方面的漏洞，以及各个设备和系统的各种端口分配、提供的服务、服务软件版本等存在的安全弱点。系统提供详尽的扫描分析报告和漏洞修补建议，帮助管理员实现对贵州省无线电管理信息系统网络，尤其是其中的重要服务器主机系统的安全加固，提升安全等级。

漏洞扫描系统提供以下功能：

漏洞扫描

漏洞知识库从操作系统、服务、应用程序和漏洞严重程度多个视角进行分类，支持对漏洞信息的检索功能，可以从其中快速检索到指定类别或者名称的漏洞信息，并具体说明支持的检索方式。

系统内置不同的策略模板如针对 Unix、Windows 操作系统等模板，同时允许用户定制扫描策略；用户可定义扫描范围、扫描使用的参数集、扫描并发主机数等具体扫描选项。

可以在扫描过程中人工指定包括 SNMP、SMB 等常见协议的登陆口令，登陆到相应的系统中对特定应用进行深入扫描。

可定义扫描端口范围、端口扫描方式，支持多种口令猜测方式，包括利用 Telnet, Pop3, Ftp, Windows SMB 等协议进行口令猜测，允许外挂用户提供的字典档。

漏洞分析

能够对扫描结果数据进行在线分析，能够根据端口、漏洞、BANNER 信息、IP 地址等关键字对主机信息进行查询并能将查询结果保存。

能够在线对多个已完成的扫描任务进行合并分析。

离线报告可以输出到 HTML、WORD、EXCEL 等文件，报告可以直接下载或通过邮件直接发送给相应管理人员。

在线报表中对综述、主机、漏洞、趋势等信息进行分类显示；综述中应对漏洞和风险分布进行定量统计分析并展示。

漏洞管理

提供 XML、SNMP TRAP 和 HTTP 等二次开发接口给其他的安全产品或者态势分析和安全运营平台调用，并且提供具体接口的说明文档。

对扫描出来的资产的安全漏洞能够发送邮件给对应的资产管理员，通知其限期内修复漏洞并自动对修复进行验证，实现对漏洞的有效跟踪和验证。

提供对资产风险的多次趋势分析能力，能够有效地分析网络整体和主机的漏洞分布和风险的趋势。

能够进行自动和手动的漏洞库升级，保证随时拥有检测最新漏洞的能力。

1.2.4.4.2 应用安全

通过网络、主机系统的安全防护，最终应用安全成为信息系统整体防御的最后一道防线。在应用层面运行着信息系统的基于网络的应用以及特定业务应用。基于网络的应用是形成其

他应用的基础，包括消息发送、web 浏览等，可以说是基本的应用。业务应用采纳基本应用的功能以满足特定业务的要求，如电子商务、电子政务等。由于各种基本应用最终是为业务应用服务的，因此对应用系统的安全保护最终就是如何保护系统的各种业务应用程序安全运行。

因此在网站系统应用软件的安全方面要考虑：身份鉴别、访问控制、安全审计、入侵防范方面的安全问题，这些问题在很大程度上由网站系统应用软件的开发商在应用软件的设计和开发阶段就需要考虑。

1.2.4.4.2.1WEB 应用防火墙

在贵州省无线电管理信息系统 WEB 服务器前端部署专业的 WEB 应用防火墙（WAF），对 WEB 应用服务和网页内容进行防护，屏蔽对网站的攻击和篡改行为，实现防跨站攻击、防 SQL 注入、防止黑客入侵、网页防篡改等功能，从而更有效地对网站服务器系统及网页内容进行安全保护，从应用和业务逻辑层面真正解决 WEB 网站安全问题。

WEB 应用防火墙应能提供以下主要功能：

WEB 应用威胁防御

支持对 HTTP 数据流进行深度分析，内置针对 WEB 攻击防护的专用特征规则库，规则涵盖诸如 SQL 注入、XSS（跨站脚本攻击）等 OWASP TOP10 中的 WEB 应用安全风险，及远程文件包含漏洞利用、目录遍历、OS 命令注入等当今黑客常用的针对 WEB 基础架构的攻击手段。

对于 HTTP 数据包内容具有完全的访问控制权限，检查所有经过网络的 HTTP 流量，回应请求并建立安全规则。一旦某个会话被控制，WAF 能对内外双向流量进行多重检查，以阻止内嵌的攻击，保证数据不被窃取。网站管理者也可以指定各种策略对 URL、参数和格式等进行安全检查。

网页防篡改

WAF 应能够监控网页请求的合法性，实时拦截篡改攻击。同时，通过比对请求页面的哈希指纹，校验被请求的网页是否被篡改。一旦检测到发生网页篡改紧急事件时，WAF 会将用户请求重定向到默认页面或指定的正常页面，使篡改攻击者的意图不能得逞。

视篡改的程度或网站特殊需求，启动专业的应急机制。一方面支持对网络流量进行有效控制，及时阻止篡改攻击行为，保证网站形象。另一方面可提供多种形式的告警机制，通知网站管理者进行事件分析和历史追溯，从而完成 WEB 服务器的配置及数据恢复，杜绝网页内容连续被篡改。

抗拒绝服务攻击

WAF 系统中集成抗拒绝服务攻击功能，能够防御迄今已知的所有种类 DDoS 攻击，如 SYN Flood、UDP Flood、ICMP Flood、ping of Death、Smurf、HTTP-get Flood 等。同时对未知攻击也能进行有效防护。主要技术包括：

攻击指纹识别：利用多种技术手段对网络数据包进行特征统计和发现，能够准确定位当前的攻击类型，并触发不同的防御机制，在提高效率的同时确保防护准确度。

异常流量识别：支持基于数据挖掘的 DDoS 攻击盲检测技术。利用关联算法和聚类算法自适应的产生检测模型，任何偏离这些正常状态的流量特征都可以被捕获，从而可以实时、自动、有效地识别出异常流量。

攻击特征挖掘：具备高效的攻击特征挖掘能力。系统通过对网络流量的显微分析，挖掘出攻击特征，并将攻击特征移交给规则执行机进行高效执行。

攻击流量过滤：针对检测出的攻击流量，采用规则执行机技术，准确彻底地过滤攻击流量，放行正常流量，保证网站服务的正常进行。

WEB 应用漏洞扫描

WAF 提供对网站应用漏洞的扫描功能。该功能基于先进的漏洞扫描引擎及庞大漏洞信息库。扫描内容涵盖： SQL 注入、跨站脚本编制及操作系统命令注入等 WEB 常见漏洞。扫描任务支持单任务及批量任务。执行方式可按时间周期进行灵活设置。扫描结束后，自动生成全中文网站漏洞分析报告。此功能可以使网站管理者在不需要安装任何漏洞扫描软件的情况下，直观地了解到网站存在的安全漏洞情况，以及时进行相关修补工作。

WEB 应用加速

WAF 在对网站进行全面的安全防护的同时，通过连接池、缓存等机制，实现应用加速，优化网站性能的功效。

WEB 应用加速功能通过高性能的硬件平台及软件加速算法，可以将用户的 WEB 请求响应速度提高数倍，大幅提升网站系统的可用性。

业务智能分析

WAF 提供强大的网站业务智能分析功能。内容丰富，涵盖网站业务数据智能分析、网站安全数据智能分析以及网站管理数据智能分析三大模块。展现形式为数据表格搭配统计图示，效果清晰、直观。为网站管理者提供有针对性的决策依据。

网站业务数据智能分析：提供强大的网站业务统计分析功能。针对网站管理者希望了解到的网站业务参数指标，TopWAF 按照不同时间段、不同地区及不同内容，分别对网站

流量、网站访问者以及网站内容进行统计分析。统计内容专业、准确，完全可以替代市面上的网站业务监测软件。

网站安全数据智能分析：对来自于边界的各种攻击行为进行详细记录。通过 WEB 攻击日志、DDOS 攻击日志、网页防篡改日志及网页敏感关键字过滤日志，将网站的安全现状直观的展现给网站管理者。统计类型包括时间段、地址来源及攻击种类等，管理者可以通过分析相关数据对网站实施更有针对性的安全策略

网站管理数据智能分析：管理员操作记录是安全产品不可或缺的功能，WAF 应提供告警统计及监控统计报表功能。系统会自动记录所有的报警事件及监控状态，为网站管理者提供良好的管理凭证。

1.2.4.4.2.2 无线电管理平台防护系统

在无线电管理信息系统配置一套无线电管理防护系统，能实现对无线电管理一体化平台进行防护，持续保障无线电管理一体化平台稳定运行，为避免因兼容性问题导致无线电管理一体化平台系统功能异常、数据丢失等安全问题，无线电管理平台防护系统应与无线电管理一体化平台兼容。

资产清点：通过设置检查规则，系统自动检查已安装探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备；针对不同网络状况，提供多种探查方法，包括“ARP 缓存分析”、“Ping 扫描”、“Nmap 扫描”、“连接记录分析”等，客户可灵活选择；功能基于实际业务环境发现主机，减少无意义网络资源消耗，保证探测与被探测主机正常运转。

应用清点：自动化清点进程、端口、账号、中间件、数据库、大数据组件、Web 应用、Web 框架、Web 站点等十余类安全资产，覆盖通用资产；根据每个服务器业务特点，系统针对性识别应用。

风险发现：在资产细粒度清点的基础上，持续、全面透彻地发现潜在风险及安全薄弱点，根据多维度的风险分析和精确到命令行的处理建议，用户可及时处理重要风险，以限制黑客接触系统、发现漏洞和执行恶意代码，从而大大提高系统的攻击门槛。持续性监测所有主机的安全状况，图形化展现风险场景。主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险，帮助单位快速有效解决潜在威胁。

入侵检测：通过多维度的感知网络叠加能力，对攻击路径的每个节点都进行监控，并提供跨平台多系统的支持能力，保证了能实时发现失陷主机，对入侵行为进行告警。不依赖

对漏洞黑客工具的了解，有效发现未知黑客攻击，通过对用户主机环境的实时监控和深度了解，有效发现包括“0day”在内的各种未知黑客攻击。通过 Agent 以其轻量高效的特性，在保证对用户主机安全监控的前提下，不对其业务系统产生影响，为用户的主机安全提供了高效可靠的保护。

威胁快速响应：高效的安全事件响应措施，通过端口安全防护、暴力破解防护、入侵扫描防护、IP 黑白名单、进程行为控制、进程白名单、勒索诱捕、病毒查杀等响应措施高效处置安全威胁，图形化展示各类攻击事件，提供立体化的安全防护能力。

无线电管理一体化平台兼容性：无线电管理平台防护系统为无线电管理一体化平台提供持续稳定的防护能力，与无线电管理一体化平台应用兼容适配。兼容性主要体现在无线电监测平台涉及的数据库、中间件、API、数据格式、传输协议、无线电监测平台软件版本、部署环境等内容。

1.2.4.4.3 数据安全及备份恢复

信息系统处理的各种数据（用户数据、系统数据、业务数据等）在维持系统正常运行上起着至关重要的作用。一旦数据遭到破坏（泄漏、修改、毁坏），都会在不同程度上造成影响，从而危害到系统的正常运行。由于信息系统的各个层面（网络、主机、应用等）都对各类数据进行传输、存储和处理等，因此，对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。各个“关口”把好了，数据本身再具有一些防御和修复手段，必然将对数据造成的损害降至最小。

另外，数据备份也是防止数据被破坏后无法恢复的重要手段，而硬件备份等更是保证系统可用的重要内容，在高级别的信息系统中采用异地适时备份会有效的防治灾难发生时可能造成的系统危害。

保证数据安全和备份恢复主要从：数据完整性、数据保密性、数据备份恢复、剩余信息保护和个人信息保护等方面予以考虑。

1.2.4.4.3.1 数据传输完整性和保密性（VPN）

对于贵州省无线电管理信息系统注册用户及移动办公、远程运维人员通过边界登录到网站系统进行的业务交互操作或远程管理操作，通过部署 SSL VPN 网关设备，采用基于预留信息+手机短信或基于 PKI 数字证书的认证机制实现用户身份认证，利用对称密钥技术实现数据传输的保密性和完整性，并采用数字签名技术保证交易的抗抵赖性，可方便地实现应用系统用户的远程安全访问，保证重要、敏感信息在网络传输过程中完整性和保密性。

SSL VPN 网关主要功能包括：

符合国密局技术规范和算法要求：全面支持国家密码管理局制定的《SSL VPN 技术规范》，支持多种国内自主研制的硬件密码算法，采用硬件密码模块进行密码算法运算，支持国家密码管理局规定的 SM2、SM3、SM4 商用密码算法。可选支持国际通用协议和算法。

支持多种 SSLVPN 技术实现应用全覆盖：同时支持三类主要的 SSLVPN 接入技术：WEB 转发（WEB FORWARD），端口转发（PORT FORWARD）和全网接入（NETWORK ACCESS 或者称为 IP TUNNEL），用户可以根据自身应用系统的特点选择使用一种或多种接入方式。

WEB 转发模式可以实现用户的完全无客户端接入，支持各种操作系统和客户浏览器平台。

端口转发模式通过客户端本地代理技术实现对用户访问请求的 SSL 协议封装和转发。

全网接入模式通过 SSL 隧道转发客户端所有的 IP 请求报文，其适应性最好，能够支持基于 IP 协议的所有 B/S 和 C/S 业务系统，其同样要求在客户端系统上安装一个 ACTIVEX 的控件。

支持丰富的认证机制：支持丰富多样的内外部认证支持，能与用户原有认证系统无缝结合，保障业务延续性；内置短信认证模块，杜绝口令泄露；支持硬件特征码认证，保障使用身份；动态令牌认证，口令一次一变；支持各种认证随意组合，提供最强的安全认证机制；提供差异化的认证方式，给用户提供多种选择。

全面支持标准 PKI/CA 体系：支持既能够通过内置的 CA 模块独立为移动用户签发数字证书，又能够通过导入 CA 根证书＋CRL 列表方式对第三方 CA 签发的证书进行认证，同时还能够通过 OCSP/LDAP 等标准协议向第三方 CA 提交在线证书认证请求。

支持灵活安全的资源授权：支持多级授权机制和用户授权继承的策略，满足各种用户授权需求。支持整体授权、条件授权、属性授权；支持基于证书的属性字段的授权；支持基于内外部属性（LDAP 或 Radius 下发属性值）的授权；还支持多条授权策略的组合。在用户授权的粒度上，支持基于 URL/目录/文件等访问内容的授权、用户行为动作的访问授权、基于访问时间的授权等，能够满足各种用户授权需求。

1.2.4.4.3.2 数据存储完整性和保密性（后期项目解决）

针对存储在不同位置的数据，分别采用磁盘加密、数据库加密、文件加密等手段保证重要数据在存储过程中的完整性和保密性。

1.2.4.4.3.3 服务器双机热备或集群（后期项目解决）

对于重要的网站服务器、应用服务器、数据库服务器及相应的网络路由设备和边界安全

设备，均需要采用双机热备或多机集群的部署方式提供高可用性保障。

1.2.4.4.3.4 数据备份恢复（本地备份利旧，备份后期项目解决）

业务信息系统需要进行备份的数据包括存储在各个数据库系统中的业务应用数据、监控管理数据、日志审计数据、策略配置数据等。在贵州省无线电管理信息系统数据容灾模式的选择上，建议采用以在线备份系统为主，离线备份介质为辅的方式，一方面可通过快速的数据恢复满足业务连续性的需要，另一方面也确保大量的历史数据得到经济、妥善的保存，节省在线存储设备开销。

建议采用以下组合的数据灾备方案：

本地备份（利旧现有备份设备）

通过现有备份设备对各业务系统的在线业务数据进行同步存储备份。一旦主存储系统出现故障导致数据丢失，可迅速从备份设备上进行恢复，可达到 RPO 接近于 0 的目标。

备份（后期项目解决）

在条件允许的情况下，建议采用远程异地在线备份。可通过备份机房的备份设备实现数据的远程备份，当发生不可预知性灾难时，远程存储设备能够将数据恢复，达到容灾的功能。

备份机房在安顺无线电监测站搭建，为应对各种站点级的灾难事件提供快速的恢复能力。

应用级灾难备份（后期项目解决）

鉴于重要业务信息系统对于实时性要求较高，建议在条件允许的情况下，在数据级容灾系统基础上建立应用级容灾系统，同时完成数据和应用系统环境的复制存放和管理。一旦发生灾难事件导致主中心无法再继续提供应用服务，可迅速切换到备份中心，确保关键业务的连续运行，以便继续为用户提供应用服务和数据访问，让服务请求能够透明（在灾难发生时毫无觉察）地继续运行。

为实现发生灾难时的快速应用切换，灾备中心的备份系统应配置与主中心工作系统同构和相同功能的业务网络、应用服务器、应用软件等，当然为了节省资金，灾备中心的通信链路和网络设备、主机系统等暂可不采用冗余和集群部署，将来根据需要再行扩充。当主中心的工作系统出现不可恢复的物理故障时，应立即切换至备份中心的容灾系统，并将备份数据挂接到备用系统上，尽快恢复业务运行。待主中心修复后，备份中心向主中心进行反向同步和回切，从而实现主中心的完全修复和恢复运行。

1.2.4.4.3.5 剩余信息保护（登录设备时功能设置，无需设备）

为保证存储在硬盘、内存或缓冲区中的信息不被非授权的访问，操作系统应对这些剩余信息加以保护。用户的鉴别信息、文件、目录等资源所在的存储空间，操作系统将其完全清

除之后，才释放或重新分配给其他用户。

采取的措施包括：

取消操作系统、数据库系统和堡垒机等系统的用户名、登录密码自动代填功能。

采用数据擦除工具，确保身份鉴别信息和敏感业务数据所在的存储空间被释放或重新分配前得到完全清除。

1.2.4.5 安全管理中心设计

1.2.4.5.1 三员管理（运维安全审计）

安全管理中心应做到系统管理员、安全保密管理员和安全审计员的三权分立，并对各类管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行权限范围内的管理操作，并对这些操作进行审计。

系统管理员：主要负责系统的日常运行维护工作。包括网络设备、安全保密产品、服务器和用户终端、操作系统数据库、涉密业务系统的安装、配置、升级、维护、运行管理；网络和系统的用户增加或删除；网络和系统的数据备份、运行日志审查和运行情况监控；应急条件下的安全恢复。

安全保密管理员：主要负责系统的日常安全保密管理工作。包括网络和系统用户权限的授予与撤销；用户操作行为的安全设计；安全保密设备管理；系统安全事件的审计、分析和处理；应急条件下的安全恢复。

安全审计员：主要负责对系统管理员和安全保密员的操作行为进行审计跟踪、分析和监督检查，及时发现违规行为，并定期向系统安全保密管理机构汇报情况。

1.2.4.5.2 集中日志收集与分析（日志审计）

在安全管理区部署一套集中的日志收集和分析系统，通过被动采集（SYSLOG、SNMPTRAP）或主动采集（ODBC/JDBC、文件读取、安装 AGENT）的方式对贵州省无线电监测站政务云数据中心网络中所有网络设备、服务器操作系统、应用系统、安全设备、安全软件管理平台等所产生的日志数据进行统一采集、存储、分析和统计，为管理人员提供直观的日志查询、分析、展示界面，并长期妥善保存日志数据以便需要时查看。保证审计记录的留存时间符合法律法规要求。

集中日志审计系统实现以下功能：

日志收集：收集用户内、外网的网络设备、安全设备、服务器、数据库以及采取 B/S 方式进行开发的各类应用系统，进行统一集中存储和汇总，并提供给系统管理人员进行进一步的分析和查询；

日志归一化处理：将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者。

原始日志高效存储：完备的原始日志数据存储策略，符合塞班斯、等保、分保等合规性要求。管理者可以针对不同的管理对象设置不同的存储策略。采用专用数据存储技术对海量安全信息数据进行实时压缩，压缩比高达 10:1，每兆存储空间可存储 20000 条以上安全信息，数据加密存储，防篡改。支持自定义存储位置（磁盘阵列、SAN、NAS 等内外部存储网络）以获取超大存储空间。支持存储空间实时动态监视，图形化显示最新存储空间使用情况。支持按存储空间、存储时间进行多维度存储策略管理。若存储空间超过设定阀值则系统自动报警，提醒管理者备份原始数据。数据的备份支持手动备份、自动备份两种模式。

日志查询：支持对海量日志信息进行组合条件检索查询，独特的海量数据查询技术，真正实现了即查即显。查询结果根据归一化后的格式展现给管理者，便于管理者事后追溯。同时为具有一定专业知识的高级管理者提供归一化日志与原始日志同屏对比显示功能，高级管理者可以更深入的分析原始日志数据。支持多条件日志检索查询；支持原始日志全文检索。查询结果支持 word、pdf 等多种格式导出；支持将备份日志数据进行还原检索查询；支持查询结果二次查询。

统计分析报表：系统在对安全信息数据进行详尽的分析及统计的基础上支持丰富的报表，实现分析结果的可视化。为了帮助管理员对网络事件进行深度的挖掘分析，系统内只多种统计主题，支持管理员从不同角度进行安全信息的可视化分析。审计报表支持按照排行、流量和概要进行统计，同时支持日、月、年等统计周期。对于统计结果系统提供了表格及多种图形表现形式（柱状图、曲线图），使管理员一目了然。

报警管理：日志审计系统可以定义事件的报警方式，即定义什么样的事件采取什么样的报警方式，另外系统管理人员利用日志审计系统，也可以定义自动告警功能，而且用户可以自定义告警内容及管理员应采取的措施，保证报警信息能够足以提醒安全保密管理人员有安全事件发生。

1.2.4.5.3 防病毒管理（利旧）

利旧现有的杀毒软件，确保全网具有一致的防病毒策略和最新的病毒查杀能力。安全管理员负责防病毒软件的总体维护，定期检查防病毒服务器的运转情况，如有异常及时处理。系统管理员有责任维护各应用服务器及终端防病毒系统的正常运转，也需要定期对防病毒软件的升级情况进行监控。如果遇到问题或者病毒报警，与安全管理员共同解决。

1.2.4.5.4 补丁管理（利旧服务器）

通过利旧现有服务器搭建补丁服务器，针对厂商最新发布的补丁或针对已发现漏洞的补丁及时进行更新，确保全网具有一致和最新的漏洞修复能力。

部署的补丁服务器，可以设定补丁更新的时间，服务器端下载完补丁后，可以在设定的时间点向客户端推送补丁。并且补丁服务器与厂商最新发布的补丁同步时间也可以设定，这样可以确保不在工作时间因同步补丁而占用带宽，影响终端用户使用网络的情况。设置补丁服务器自动与厂商补丁服务器同步，补丁自动实时更新，不会发生补丁漏更的情况。

1.2.4.5.5 态势感知平台

态势分析和安全运营平台是为贵州省无线电监测站网络信息安全应急保障工作提供支撑的技术平台，实现收集、关联和实时分析各种网络安全监测数据，通过高效专业化支撑平台和先进监测工具及时发现、识别安全事件，及时掌握安全状态，了解覆盖整个网络的网络攻击、病毒传播和异常行为等网络安全事件，为预警、应急响应和事件调查提供支撑。

态势分析和安全运营平台实现对全网环境下的整体信息资产、安全事件、安全风险、访问行为等的统一分析与监管，通过关联分析技术，使系统管理人员能够迅速发现问题，定位问题，有效应对安全事件的发生。主要用到的安全管理技术有：网络监控、安全认证管理、安全策略管理、安全监控管理、安全事件管理、系统资源管理、流量分析管理等。

在安全管理区部署态势分析和安全运营平台，提供对全网安全事件的集中监控、分析和处置，以及对安全风险、安全发展态势的集中监测，对整个网络进行集中的安全管理，对安全事件进行深度分析，并快速做出智能响应，最终实现对信息系统安全风险的集中监管，提升贵州省无线电管理信息系统的安全运维能力，更好地支撑业务持续性发展。

态势分析和安全运营平台依据 ISO 27001 安全管理标准，结合安全服务的最佳实践，以风险管理为核心，通过深度数据挖掘、事件关联等技术，实现了网络内部各类安全事件的集中管理和智能分析，提供多视角、实时动态的风险现状展示。同时，系统内置了多种报警响应、工单机制以及专家建议系统，可以帮助用户采取及时、有效的安全措施以实现闭环的、持续改进的网络安全管理，保证用户的业务不受影响。

态势分析和安全运营平台主要功能包括：

资产信息管理

实现对信息系统内所有的 IT 资产信息进行集中统一的管理，包括资产的特征、分类等属性；但同时资产信息管理并不是为了简单的统计，而是在统计的基础上来发现资产的安全状况，并纳入到平台的数据库中，为其它安全管理模块提供信息接口。

安全事件管理

通过实时采集、过滤、汇聚、关联分析等手段充分缩减信息系统中时刻产生的海量安全事件信息，并对安全事件进行严重性排序，优先呈现和处理严重性级别较高的安全事件，以便了解系统实时的安全事件状况。关注的事件类型包括攻击行为、异常活动和状态、病毒以及安全告警等。

安全风险管理

基于资产管理、事件管理和评估管理，根据风险的三要素（资产、威胁、弱点），从单个资产、业务系统、安全域、物理地域等多个维度自动分析和呈现信息系统的安全风险状况。

脆弱性管理

实现对重要信息资产安全脆弱性（漏洞、配置缺陷等）的收集和管理。提供两种方式：通过远程安全扫描获得安全脆弱性信息和通过人工评估的方式收集脆弱性信息。在定期收集到这些脆弱性信息后可以利用脆弱性管理系统进行导入和处理，以利于安全管理员对脆弱性信息的查询、呈现并采取相应的措施进行处理，将单点脆弱性转化为全局脆弱性感知。同时通过集中化脆弱性治理概念，使用工单机制，将发现的脆弱性及时进行补丁更新或配置加固，实现脆弱性全生命周期处理流程可审计，进而实现全生命周期脆弱性管理。

安全预警管理

管理并实时呈现信息系统中的各类安全威胁、安全风险、安全态势、安全隐患等信息，在统一界面上给出网络安全的趋势分析报表，分析的内容包括漏洞的分布范围、受影响的系统情况、可能的严重程度等；根据全网安全事件的监控情况，在统一界面上给出现网中主要的攻击对象分布、攻击类型分布等情况分析，指导全网做好有效的防范工作，防止类似事件的发生；提供接收风险数据的接口，预先定义数据格式，自动生成预警信息。

安全响应管理

主要是提供安全事件响应流程和响应方式的管理。提供专家系统和知识库的支持，针对各类安全管理人员所关心的安全问题进行响应。响应方式包括从专家系统调用相关脚本自动进行漏洞修补、防火墙配置下发、网络设备端口关闭等操作，从知识库自动/手动的进行解决方案的匹配，然后通过自动或手动产生工单，通知相关管理员进行处理，并对工单的生命周期进行监控，此外还包括利用短信、Email 等方式进行通知等。

安全处置管理

联动现有无线电监测终端安全防护系统处置安全事件，保障无线电监测终端网络安全。无线电监测终端作为单位重要资产，终端安全防护系统提供重要资产的全生命周期安全防护，联动处置作为一项重要的安全防护手段，态势感知系统支持与无线电监测终端安全防护系统

兼容适配，兼容性主要体现在一键安全威胁扫描、一键恶意文件隔离、安全策略联动。

联动本次项目新增的防火墙系统处置安全事件，保障无线电信息管理整体网络安全。

联动全威胁检测系统处置安全事件，保障整体数据流量安全。

联动漏扫，及时识别资产漏洞，保障资产安全。

安全工单管理

主要实现安全工单的产生及流转，并依此实现安全管理人员的工作考核。

安全知识管理

安全知识管理包括对事故案例库、解决方案库、补丁程序库、专家知识库等的建立和管理以及安全事件发布和安全知识的培训和考试。

1.2.5 安全管理体系设计

“三分技术，七分管理”这句话是对网络安全保密工作非常客观的描述。任何安全保密仅在技术上是做不到完整的安全，还需要建立一套科学、严密的网络安全管理体系，为计算机信息化网络系统提供制度上的保证，将由于内、内外部的非法访问或恶意攻击造成的损失减少到最小。因此不能忽视安全保密管理，必须提供具体的安全保密管理措施。

根据安全防范体系中的各种安全技术所需的技术管理工作，设定安全管理的角色：业务系统管理员、网络系统管理员、安全保密管理员、密钥管理员、系统审计员等职位。根据不同的职能，定义不同角色的责任和权利，制定相应的操作规范。

本项目免费运维期内的安全管理体系支撑工作由项目承建商免费提供，免费运维期满后的安全管理体系支撑工作由运维服务商提供。

1.2.5.1 安全管理机构设计

安全管理机构的规划，应以安全组织架构设计为基础，定义架构中涉及到的科室和岗位的职责以及管理方法，其内容包含但不少于等级保护基本要求中的第 3 级信息系统的管理要求中对管理机构的要求。

根据其在信息安全工作中扮演的不同角色进行优化组合的结果，反映了各科室在信息安全工作中的不同定位和相互协作关系。信息安全组织架构主要包括参与信息安全决策、管理、执行和监督工作的科室。

信息安全组织架构包含以下三个关键要素：

决定了信息安全工作中正式的报告关系，包括层级数和管理者的管理跨度；

决定了如何由个体组合成科室，再由科室到组织；

组织架构中包含了一套系统，以保证跨科室的有效沟通、合作与整合。

信息安全组织架构是开展信息安全工作的基础。在日常管理过程中，存在着多项信息安全管理事宜，需要对其中的重要事件进行决策，从而为信息安全管理提供导向与支持；对于所制定的信息安全管理方针需要进行有效的贯彻和落实；另外，对信息安全管理方针贯彻落实的情况还需要进行监督，以上各种情况都需要一个完善有效的信息安全组织架构来支撑。另外在未来信息安全保障体系建立的过程中，各种信息安全项目的开展将成为信息安全工作的一项重要内容，这也需要有相应的组织予以支持。

本方案提出的信息安全组织架构是以等级保护基本要求为指导，在借鉴国际最佳实践的基础上根据信息安全工作开展的需求进行完善的结果。

在完整的信息安全组织中一般包含以下几个重要组成部分：

信息安全决策机构

信息安全管理机构

信息安全执行机构

信息安全监管机构

以上组织机构的具体存在形式可以是多样的，如兼职的、虚拟的或者远程的。目前国际上普遍采用的信息安全组织架构如下图所示：

图 5.2-3 信息安全组织架构图

信息安全决策机构

信息安全决策机构处于整个信息安全组织架构的顶端，主要从高层领导的角度对于信息安全方面的工作进行指导和控制，信息安全决策机构应当是安全工作的最高决定者，主要职能包括：

1)确定信息安全工作的战略和方向

2)决定本项目信息安全组织

3)总体调配信息安全工作的资源

4)负责通过和决定信息安全策略和标准

5)对于信息安全方面的重大项目进行审批

6)在协调安全工作中协调各科室关系

一般信息安全决策机构在组织中的主要表现形式是由相关各科室主管负责人或代表组成的的信息安全领导委员会，参与人员主要取决于需要决策的内容。信息安全决策机构需要对信息安全工作开展中的重大事项进行决策，因此必须要有信息安全专职管理机构的代表；

信息安全工作的需求来自于业务的开展，因此很多情况下也考虑各科室的代表的参与；信息安全决策工作中的一项重要课题是资源保障，因此往往需要分别拥有资金调配、人员调配和设备调配权力的科室的代表。至于对各科室选派代表的要求取决于决策机构的工作形式，一般来说需要有相关决定权力的人员作为代表。

信息安全管理机构

信息安全管理机构是整个信息安全管理体系建立和维护的组织者和管理者，它同时具有两种角色：

1）信息安全管理机构是信息安全决策机构的决策支持者，由管理机构为决策机构提供必要的决策所需信息；

2）信息安全管理机构是信息安全工作的规则制定者和决策推行的管理者。可以说是信息安全决策机构的执行组织，也可以说是信息安全执行机构的管理组织。

信息安全管理机构的职能主要包括：

1）整个贵州省无线电管理信息系统信息安全相关政策标准的制定、更新

2）信息安全项目的规划、评审和质量控制

3）对信息安全工作的开展进行日常管理和监督

信息安全执行机构

信息安全执行机构主要负责具体信息安全工作的执行和开展。一般信息安全执行机构主要包括信息安全工程组织和信息安全运行组织两大类的组织。信息安全工程组织一般以独立项目小组的形式存在，由专门的信息安全开发和工程科室和相关工程人员组成。

信息安全工程组织主要负责的工作包括：

1.信息安全基础建设

包括各项信息安全技术的实施，如认证授权与访问控制系统的建设，信息安全运营中心的建设等

2.信息安全管理项目实施

信息安全管理项目的实施也是信息安全工程组织的重要工作之一，例如信息安全规划，信息资产识别与风险评估，信息安全标准与规范的制定等。

对于信息安全运行组织在贵州省无线电管理信息系统中主要负责日常信息系统监控维护方面的工作，并及时汇报日常运作中信息系统的安全情况。信息安全运行组织一般是一个虚拟的机构，包括运行维护、监控和技术支持在内的专职或兼职的信息安全人员，通常会分散安排在各个相关科室中，并统一向专门的信息安全运行管理人员汇报和负责。除此之外，

专门的信息安全运营中心或是由外包商提供的监控服务也属于这一机构的范畴内。信息安全运行组织的主要职责可以概括如下：

1）依照各项管理政策、标准与规范、指南与细则开展工作

2）提供各种安全服务以直接支持业务，包括监控、事件响应、故障处理等

3）将工作中的各种需求和重要事项汇报给信息安全管理机构

4）接受管理机构和监督机构的监管、控制，并配合其开展工作

信息安全监管机构

信息安全监管机构的主要职能是对贵州省无线电管理信息系统内信息安全工作的开展情况进行独立的审查和监督。它可以是贵州省无线电管理信息系统的内部审计科室，也可以是独立的内外部第三方审计机构，其主要职责如下：

1）监督各项信息安全策略、标准与规范、指南与细则的执行情况，检验信息安全管理机构和执行机构是否按照其开展工作。

2）检验信息安全管理机构和执行机构的工作效果，包括信息安全项目审查、信息安全服务效果审查，总体信息安全情况评估和信息系统安全性评价等工作。

信息安全监管机构是针对贵州省无线电管理信息系统信息安全管理机构和执行机构的工作进行监管，其审查监督的结果直接向信息安全决策机构或者贵州省无线电管理信息系统的决策层进行汇报，为信息安全组织改进工作提供支持。

信息安全角色和职责

从根本上来说，信息安全是贵州省无线电管理信息系统中每一个和信息系统相关或是能影响信息系统的安全情况的人员的职责。每个人在信息系统的运行中，在不同岗位上都扮演着相应的角色。本部分将定义出贵州省无线电管理信息系统中与信息安全工作相关的主要角色，并从总体上描述他们所承担的职责。

在信息安全工作方面一直在进行讨论的一个基本问题就是“到底是谁的职责？”，许多人对于信息安全相关职责仍停留在传统概念中，认为信息安全是信息技术科室或仅仅是信息安全科室的职责，这样给信息安全工作的开展带来了很大的困难。通过定义信息安全角色与职责，使贵州省无线电管理信息系统中每个工作人员都能找到自己的位置，同时为以后具体岗位职责的定义打下了坚实的基础。

通常在信息安全相关的角色主要包括几下几种：

1)高层管理人员

2)信息安全管理人员

3)科室和项目管理者/应用所有者

4)技术提供、维护和支持人员

5)管理支持者

6)用户

由于各自的角色不同他们在信息安全方面也承担着不同的职责。

1.2.5.1.1 信息安全领导小组

高层领导参加的信息安全领导小组，负责批准信息安全策略、分配安全责任并协调整个贵州省无线电管理信息系统范围的安全策略实施，确保对安全管理和建设有一个明确的方向并得到管理层的实际支持。信息安全领导小组应通过合理的责任分配和有效的资源管理促进贵州省无线电管理信息系统网络信息系统的安全。信息安全领导小组可以作为目前管理机构的一个组成部分。

信息安全领导小组有如下职责：

1)就整个科技处的信息安全的作用和责任达成一致；

2)审查和批准信息安全策略以及总体责任；

3)就信息安全的重要和原则性的方法、处理过程达成一致，并提供支持。如风险评估、机密信息分类方法等；

4)确保将安全作为制定业务建设和维护计划、内部信息系统建设的一个部分；

5)授权对安全控制措施是否完善进行评估，并协调新系统或新服务的特定信息安全控制措施的实施情况；

6)审查重大的信息安全事故，并协调改进措施；

7)审核信息安全建设和管理的重要活动，如重要安全项目建设、重要的安全管理措施出台等；

8)在整个组织中增加对信息安全工作支持的力度。

1.2.5.1.2 信息中心

负责设计、建设安全管理体系，包括策略、组织和运作模式，并且进行宣贯和培训。

信息中心有如下职责：

1)贯彻执行政府相关主管科室有关网络及信息安全管理方面的方针、政策及各项工作要求，在各网上落实网络及信息安全的各项工作。通过等级保护工作保持与公安机关的联系，接受和执行公安机关的监督和指导。

2)负责建立信息安全策略体系，制定网络及信息安全工作制度及管理流程，起草、制定

网络及信息安全的技术规范、标准及策略，聘请内外部专家对网络及信息安全工作制度及管理流程进行评审，组织在全网范围内的实施。

3)组织、协调内部各科室实施网络及信息安全工作。

4)在贵州省无线电管理信息系统内开展信息安全知识共享，建立有针对信息安全的知识共享的技术平台，促进内部交流与学习。

5)定期组织内部人员或聘请内外部单位，公安机关等进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；汇总安全检查数据，形成安全检查报告，并对安全检查结果在安全组织内召开会议进行通报。

1.2.5.1.3 安全维护组

负责项目日常安全维护工作，包括信息安全专员和各科室信息安全助理。

安全维护组有如下职责：

1.执行有关信息安全问题的处理

1)在日常维护中发现有安全问题，首先进行应急处理保证业务的连续性，然后通过提供安全事件报告的方式通知安全维护组相关人员，安全维护组人员在接到报告后，将和各专业组一起在保证业务正常运行的前提下解决安全问题，工作结束后，将由双方一起记录安全处理过程；

2)对重点主机系统的安全职责；

3)至少每月进行一次安全漏洞扫描；

4)对主机系统和网络设备上的用户进行审核，发现可疑的用户账号时及时向系统管理员核实并作相应的处理。

2.对网络设备的安全职责

1)监督信息安全管理机构制订的网络设备用户账号的管理制度的实行，在发现有可疑的用户账号时向网络管理员进行核实并采取相应的措施；

2)根据业务保护要求，提出防火墙系统的部署方案，并制订相应的信息安全访问控制策略。

3.对数据库的安全职责

1)协同数据库管理员对对数据库系统进行安全配置，修补已发现的漏洞；

2)协同数据库管理员对于数据库安全事件处理，并分析安全事件原因；

3)协同数据库管理员对于数据库安全事件进行处理，尽量减小安全事故和安全事件造成的损失，并从中吸取教训；

4)验证数据备份策略的有效性，对数据恢复过程进行试验，确保在发生安全问题时能够从数据备份中进行恢复；监督数据库管理员对重要数据的备份工作，对于重要数据的备份，必须每个月做一次检查，确保备份的内容和周期以及备份介质的保存符合有关的规定。

1.2.5.1.4 安全审计组

对用户的各种行为进行审计，对安全监控中心的各项监控、处理和维护工作进行审计。

安全审计组有如下职责：

1)依赖安全运行管理平台以及各种安全审计产品对管理网的用户行为进行审计。

2)对安全监控中心的各项监控、处理和维护工作进行审计。

1.2.5.1.5 安全监控中心

可利用现有的本项目安全信息管理平台，对网络进行全面的安全监控。

安全监控中心有如下职责：

1)查看安全运行管理平台的各种告警，做出处理判断，并编制下发工单。

2)定期查看信息安全站点的安全公告，跟踪和研究各种信息安全漏洞和攻击手段，在发现可能影响信息安全的安全漏洞和攻击手段时，及时做出相应的对策，通知并指导系统管理员进行安全防范。

3)跟踪信息系统系统中使用的操作系统和通用应用系统最新版本和安全补丁程序的发布情况，在发现有新版本或者安全补丁出现发布时，通知并指导系统管理员进行升级或打补丁。

4)根据信息中心提出的安全标准，对主机系统上开放的网络服务和端口进行检查，发现不需要开放的网络服务和端口时及时通知系统管理员进行关闭；

5)定期对主机的网络服务进行全面安全检测，在发现安全设置不当或存在安全漏洞时及时通知系统管理员进行修补；

根据安全管理机构规定的周期和时间，对网络设备进行全面信息安全扫描，发现安全网络设备上存在的异常开放的网络服务或者开放的网络服务存在安全漏洞时及时通知网络管理员采取相应的措施。

1.2.5.2 安全管理人员设计

1.2.5.2.1 人员录用

1)人员录用的应以《信息安全工作人员安全管理办法》为标准：对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握安全管理基本知识；对信息系统关键岗位的人员还应注重思想品质、历史方面的考察；

2)在签署劳动合同前，应由人力资源部进行人员背景、资质审查，技能考核等，合格者还要签署《工保密协议》方可上岗；安全管理人员应具有基本的系统安全风险分析和评估能力；

3)关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员，必要时可按机要人员条件配备。

1.2.5.2.2 人员离岗

1)人员离岗的应以《信息安全工作人员安全管理办法》为标准：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所有相关证件、徽章、密钥、访问控制标记等；收回机构提供的设备等；

2)调离后的保密要求：管理层和信息系统关键岗位人员调离岗位，必须经贵州省无线电监测站人力资源部门严格办理调离手续，承诺其调离后的保密要求；

3)离岗的审计要求：涉及组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在审查合格后，方可调离；

4)对于在组织内进行岗位调动的工作人员，须根据新岗位的需要，增加、删除或修改该人员的计算机信息系统访问权限，包括电子邮件系统、业务应用系统、网络系统和其他计算机信息软硬件系统。与原岗位有关的所有资料文件，包括其软硬拷贝都需要移交，不允许私自带走。

1.2.5.2.3 安全意识教育和培训

1)定期的人员考核：应定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考；

2)定期的人员审查：对关键岗位人员，应定期进行审查，如发现其违反安全规定，应控制使用；

3)管理有效性的审查：对关键岗位人员的工作，应通过例行考核进行审查，保证安全管理的有效性；并保留审查结果；

4)全面严格的审查：对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施。

5)应知应会要求：应让信息系统相关工作人员知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；

6)有计划培训：制定并实施安全教育和培训计划，根据不同培训对象的需要，每季度或每半年进行安全培训，培养信息系统各类人员安全意识，并提供对安全政策和操作规程的认

知教育和训练等；

7)针对不同岗位培训：针对不同岗位，制定不同的专业培训计划，包括安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等；

8)按人员资质要求培训：对所有工作人员的安全资质进行定期检查和评估，使相应的安全教育成为组织机构工作计划的一部分；

9)培养安全意识自觉性：对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉存在。

1.2.5.2.4 内外部人员访问管理

1)应对硬件和软件维护人员，咨询人员，临时性的短期职位人员，以及辅助人员和内外部服务人员等第三方人员签署包括不同安全责任的合同书或保密协议；规定各类人员的活动范围，进入计算机房需要得到批准，并有专人负责；第三方人员必须进行逻辑访问时，应划定范围并经过负责人批准，必要时应有人监督或陪同；

2)在重要区域，第三方人员必须进入或进行逻辑访问（包括近程访问和远程访问等）均应有书面申请、批准和过程记录，并有专人全程监督或陪同；进行逻辑访问应使用专门设置的临时用户，并进行审计；

3)关键区域管理要求：在关键区域，一般不允许第三方人员进入或进行逻辑访问；如确有必要，除有书面申请外，可采取由机构内部人员带为操作的方式，对结果进行必要的过滤后再提供第三方人员，并进行审计；必要时对上述过程进行风险评估和记录备案，并对相应风险采取必要的安全补救措施。

1.2.5.3 安全管理制度设计

帮助用户建立起以信息安全方针、安全策略、安全管理制度、安全技术规范以及流程为一体的信息安全管理制度体系。

安全管理制度的建设，需要对贵州省无线电管理信息系统的业务和日常运营等情况非常熟悉，根据贵州省无线电监测站实际情况以及等级保护管理要求制定完整的安全管理体系。

1.2.5.3.1 规章制度

1)《信息安全组织体系和职责》：规定贵州省无线电管理信息系统安全组织机构的职责和工作。

2)《信息安全岗位人员管理办法》：加强内部人员安全管理，依据最小特权原则清晰划分岗位，在所有岗位职责中明确信息安全责任，要害工作岗位实现职责分离，关键事务双人临岗，重要岗位要有人员备份，定期进行人员的安全审查。

3)《信息安全工作人员安全管理办法》：工作人员在录用、调动、离职过程中的信息安全管理，提出对信息安全培训及教育、奖励和考核的要求。

4)《信息安全培训及教育管理办法》：贵州省无线电管理信息系统各层面信息安全培训的要求和主要内容。

5)《信息安全第三方人员安全管理办法》：必须加强第三方访问和外包服务的安全控制，在风险评估的基础上制定安全控制措施，并与第三方贵州省无线电管理信息系统和外包服务贵州省无线电管理信息系统签署安全责任协议，明确其安全责任。

6)《安全检查及考核管理办法》建立安全检查制度和安全处罚制度，对违反规章制度的科室和人员按照规定进行处罚。

7)《信息安全体系管理办法》：建设完整安全体系，实现从设计、实施、修改和维护生命周期的安全体系自身保障。

8)《信息安全策略管理办法》：安全策略本身应规范从创建、执行、修改、到更新、废止等整个生命周期的维护保障。

9)《信息安全安全现状评估管理办法》：信息安全体系的建设和维护，要通过及时获知和评价信息安全的现状，通过对于安全现状的评估，实施信息安全建设工作，减少和降低信息安全风险，提高信息安全保障水平。

10)《信息安全信息资产管理办法》：必须加强信息资产管理，建立和维护信息资产清单，维护最新的网络拓扑图，建立信息资产责任制，对信息资产进行分类管理和贴标签。

11)《信息安全 IT 设备弱点评估及加固管理办法》：增强主机系统和网络设备的安全配置，应定期进行安全评估和安全加固。

12)《信息安全预警管理办法》：对安全威胁提前预警，及时将国内外安全信息通知贵州省无线电管理信息系统各级信息安全管理人员及工作人员，确保能够及时采取应对措施，以此降低贵州省无线电管理信息系统的信息安全风险。

13)《信息安全安全审计及监控管理办法》：应部署网络层面和系统层面的访问控制、安全审计以及安全监控技术措施，保障业务系统的安全运行。

14)《信息安全项目立项安全管理办法》：加强项目建设的安全管理，配套安全系统必须与业务系统“同步规划、同步建设、同步运行”，加强安全规划、安全评估和论证的管理。

15)《安全运行维护管理办法》：建立日常维护操作规程和变更控制规程，规范日常运行维护操作。

16)《信息安全配置变更管理办法》：严格控制和审批任何变更行为。

17)《信息安全病毒防护管理办法》：加强贵州省无线电管理信息系统病毒防治工作，提升贵州省无线电管理信息系统病毒整体防护能力，降低并防范病毒对于贵州省无线电管理信息系统业务造成的影响。

18)《信息安全补丁管理办法》：按照补丁跟进和发布、补丁获取、补丁测试、补丁加载、补丁验证、补丁归档这一流程进行补丁安全管理。

19)《信息安全账号口令及权限管理办法》：加强用户账号和权限管理，按照最小特权原则为用户分配权限，避免出现共用账号的情况。

20)《信息安全应急响应管理办法》：制定各业务系统的应急方案，及时发现、报告、处理和记录。

1.2.5.3.2 管理流程

包括：安全管理规定中与管理流程配合使用，管理规定中会提出涉及流程的名称如下：

1)《信息安全管理流程—安全补丁管理流程》配合《信息补丁管理办法》使用。

2)《信息安全管理流程—安全策略管理流程》：配合《信息安全策略管理办法》共同使用。

3)《信息安全管理流程—安全配置变更管理流程》：配合《信息安全配置变更管理办法》共同使用。

4)《信息安全管理流程—安全事件处理流程》：配合《信息安全应急响应管理办法》共同使用。

5)《信息安全管理流程—安全体系运作流程》：配合《信息安全安全体系管理办法》共同使用。

6)《信息安全管理流程—办公网络环境第三方人员访问申请审批流程》：配合《信息安全第三方人员安全管理办法》共同使用。

7)《信息安全管理流程—办公终端安全处理流程》：配合《信息安全办公终端管理办法》共同使用。

8)《信息安全管理流程—应急响应流程》：配合《信息安全应急响应管理办法》共同使用。

9)《信息安全管理流程—账号安全管理流程》：配合《信息安全账号口令及权限管理办法》共同使用。

1.2.5.3.3 安全技术规范

1)《信息安全网络技术安全规范—IP 网络安全管理规范》：规范针对网络设备、网络结

构以及网络各类安全控制的操作，确保安全配置和过程控制的安全有效。

2)《信息安全网络技术安全规范—防火墙配置标准》：规范系统的安全配置，降低被攻击的风险。

3)《信息安全主机技术安全规范—系统安全规范》：针对主流操作系统的配置安全，确保安全配置和过程控制的安全有效。

4)《信息安全主机技术安全规范—windows 系统安全配置标准》：规范 windows 系统的安全配置，降低被攻击的风险。

5)《信息安全应用技术安全规范—应用系统安全规范》：规范应用系统在开发过程中，安全功能设定过程中的安全。

6)《信息安全数据安全规范—数据安全规范》：规范数据存储和传输过程中的安全控制。

7)《信息安全主机技术安全规范—应急技术安全规范》：规范应急计划的内容、应急流程、职责等相关应急准备。

1.2.5.3.4 保密协议

1)《第三方人员安全保密协议》；

2)《工作人员保密协议》。

1.2.5.4 安全建设管理设计

1.2.5.4.1 系统定级和备案

1)由信息化管理科室负责业务系统的定级备案工作，由内外部安全咨询服务团队提供技术支持，协助信息化管理开展系统定级备案工作；

2)明确信息系统的边界和安全保护等级；

3)以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；

4)组织相关科室和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；

5)确保信息系统的定级结果经过相关科室的批准；

制定《系统定级管理制度》，其基本内容包括：

6)明确负责系统定级的组织、岗位及职责，由信息安全领导小组总体负责，由信息中心负责定级工作；

7)编制《信息系统定级基本情况表》模板，用于说明信息系统的边界和安全保护等级；

8)编制《信息系统定级报告》模板，用于说明某个系统定为某个安全保护等级的方法和理由；

9)编制《信息系统定级专家评审意见》。

10)制定《系统备案管理制度》：

11)指定责任科室：由安全管理部负责管理系统定级的相关材料并控制这些材料的使用；

12)将系统等级及相关材料报系统主管科室备案；

13)将系统等级及其他要求的备案材料报相应公安机关备案。

1.2.5.4.2 安全方案设计

由信息化管理科室负责，由内外部安全咨询服务团队提供技术支持，开展安全方案设计工作：

1)根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；

2)组织有关单位对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

3)根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

4)组织相关科室和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，经过批准后，正式实施；

5)根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件；

6)制定《安全方案设计管理制度》

7)指定负责科室。由信息中心协同战略方案中心等有关科室负责安全方案设计；

8)规定方案设计流程、设计文档模板，包括：总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案；

9)规定《专家评审意见》模板。

1.2.5.4.3 安全产品采购

制定《安全产品采购管理制度》，具体内容有：

1)指定责任科室：由信息中心会同他有关科室负责产品采购；

2)定义采购流程：选型测试、年度审定及更新；

3)确定采购和使用安全产品的国家有关规定；

4)确定确国家密码主管科室对采购和使用密码产品的规定；

5)定义选型测试所需文档的模板。

1.2.5.4.4 外包软件开发

制定《外包软件开发管理制度》.由信息中心及有关软件开发管理科室共同负责外包软件开发管理:

1)根据开发需求检测软件质量；

2)软件安装之前要检测软件包中可能存在的恶意代码；

3)在合同中要求开发单位提供软件设计的相关文档和使用指南；

4)在合同中要求开发单位提供软件源代码，并审查可能存在的后门；

5)在合同中要求：在服务期内如发现安全漏洞，则开发单位必须及时提供相关安全补丁或者进行及时升级。

1.2.5.4.5 工程实施

制定《工程实施管理制度》:

1)由信息中心协同有关科室负责负责工程实施管理；

2)督促施工单位或者科室制定详细的工程实施方案控制实施过程，并按照工程实施过程进行实施；

3)维护并推行工程实施管理制度，明确说明实施过程的控制方法和人员行为准则。

1.2.5.4.6 测试验收

制定《测试验收管理制度》:

1)指定信息中心和有关科室共同负责测试验收管理；

2)委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；

3)测评单位在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

4)测评单位对系统测试验收的控制方法和人员行为准则进行书面规定；

5)由信息中心与相关科室对系统测试验收报告进行审定并签字确认。

1.2.5.4.7 系统交付

制定《系统交付管理制度》:

1)由安全管理部负责系统交付的管理工作，按照管理规定的要求完成系统交付工作；

2)制定详细的系统交付清单，根据交付清单对所交接的设备、软件和文档等进行清点。

3)对负责系统运行维护的技术人员进行相应的技能培训；

4)确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档；

5)定义系统交付控制方法和人员行为准则。

1.2.5.4.8 等级测评

制定《等级测评管理制度》：

1)指定责任单位：由信息中心负责，每年至少组织测评单位对系统进行一次等级测评，对发现的不符合项及时进行整改；

2)在系统发生变更时及时申请对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；

3)选择具有国家相关技术资质和安全资质的测评单位进行等级测评。

1.2.5.4.9 安全服务商选择

制定《安全服务商管理制度》：

1)指定责任科室：由安全管理部负责选择安全服务商；

2)确保安全服务商的选择符合国家的有关规定；

3)与选定的安全服务商签订与安全相关的协议，明确约定相关责任、服务范围、服务期限、服务各具体条款及服务质量要求等；

4)确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

1.2.5.5 安全运维管理设计

1.2.5.5.1 环境管理

制定《环境管理制度》：

1)指定责任科室：由信息中心负责环境管理；

2)定期对机房供配电、空调、温湿度控制等设施进行维护管理；

3)负责机房安全，机房安全管理人员对机房的出入、服务器的开机或关机等工作进行管理；建立《机房安全管理制度》，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；

4)规范办公环境人员行为，包括：工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的文件等。

1.2.5.5.2 资产管理

制定《资产管理制度》：

1)指定责任科室：由信息中心及有关科室共同负责资产管理；

2)编制并保存与信息系统相关的资产清单，包括资产责任科室、重要程度和所处位置等；

3)规定信息系统资产管理的责任人员或责任科室，并规范资产管理和使用的行为；

4)对信息分类与标识方法作出规定，根据资产的重要程度对资产进行标识管理，并对信息的使用、传输和存储等进行规范化管理；

5)定义管理措施选择方案：根据资产的价值选择相应管理措施。

1.2.5.5.3 介质管理

建立《介质管理制度》：

1)指定责任科室。由信息中心负责介质管理；

2)规定介质的存放环境、使用、维护和销毁；

3)由信息中心负责对存储环境进行专人管理，确保介质存放在安全的环境中，对各类介质进行控制和保护；

4)对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；

5)对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；

6)根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

7)对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

1.2.5.5.4 设备维护管理

制定《设备管理制度》：

1)指定责任科室：由信息中心及网络管理部等有关科室负责设备管理；

2)对信息系统相关的各种设备（包括备份和冗余设备）、线路等每周进行维护管理；

3)定义基于申报、审批和专人负责的设备安全管理方法，对信息系统的各种软硬件设备的选型、采购、发放、领用、维护、操作、维修等过程进行规范化管理；

4)定义配套设施、软硬件维护方面的管理方法，明确维护人员的责任，对涉外维修和服务的审批、维修过程等监督控制方法进行说明；

5)定义终端计算机、工作站、便携机、系统和网络等设备的操作和使用规范：针对主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

6)定义信息处理设备带离机房或办公地点的审批流程。

1.2.5.5.5 漏洞和风险管理

1)定期对系统进行漏洞扫描，识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；

2)定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

1.2.5.5.6 网络和系统安全管理

制定《网络和系统安全管理制度》：

1)指定责任科室：由信息中心负责网络安全管理，由信息管理科室专人负责对运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

2)对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

3)定义更新流程：根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

4)定义漏洞管理方法：定期对网络系统进行漏洞扫描，发现网络系统安全漏洞进行及时修补；

5)定义设备配置方法：实现设备的最小服务配置，并对配置文件进行定期离线备份；

6)定义内外部连接审批流程：所有与内外部系统的连接均得到授权和批准；

7)定义设备接入策略：依据安全策略允许或者拒绝便携式和移动式设备的网络接入；

8)定义非法上网管理方法：每周检查违反规定拨号上网或其他违反网络安全策略的行为。

9)指定责任科室：由信息中心负责系统安全管理，负责对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

10)根据业务需求和系统安全分析确定系统的访问控制策略；

11)每周进行漏洞扫描，对发现的系统安全漏洞及时进行修补；

12)安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；

13)依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；

14)每周对运行日志和审计数据进行分析，以便及时发现异常行为。

对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定。

1.2.5.5.7 配置安全管理

1)对记录和保存基本配置信息，包括网络拓扑结构、各个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信息进行安全管理；

2)将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。

1.2.5.5.8 恶意代码防范

制定《恶意代码防范管理制度》：

1)指定责任科室：由安全管理部负责进行恶意代码防范；

2)每年进行定期培训，通过培训提高所有用户的防病毒意识、及时告知防病毒软件版本、在读取移动存储设备上的数据以及网络上接收文件或邮件之前先进行病毒检查、对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

3)由专信息中心负责对网络和主机进行恶意代码检测并保存检测记录，每周检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报；

4)定义防恶意代码软件授权使用、恶意代码库升级、定期汇报等流程。

1.2.5.5.9 密码管理

建立《密码使用管理制度》：

1)指定责任科室：信息中心负责密码使用管理；

2)总结在密码设备的采购、使用、维护、保修及报废的整个生命周期内的各项国家有关规定；

3)严格执行上述规定。

1.2.5.5.10 变更管理

建立《变更管理制度》：

1)指定责任科室：由信息中心负责变更管理；

2)建立变更流程：确认系统中要发生的变更，制定变更方案，系统发生变更前向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，在实施后将变更情况向相关人员通告；

3)建立《变更申报和审批程序》：对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

4)建立《中止变更程序》，中止变更并从失败变更中恢复，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

1.2.5.5.11 备份及恢复管理

建立《备份及恢复管理制度》：

1)指定责任科室：由信息中心负责备份与恢复管理；

2)识别需要定期备份的重要业务信息、系统数据及软件系统等；

3)定义备份信息的备份方式、备份频度、存储介质和保存期等；

4)根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

5)建立《数据备份和恢复过程》，对备份过程进行记录，所有文件和记录应妥善保存；

6)建立演练流程：每季度对恢复程序进行演练，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

1.2.5.5.12 安全事件处置

制定《安全事件处置管理制度》

1)指定责任科室：由信息中心负责安全事件处置；

2)每年进行培训。通过培训让所有人能够报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

3)制定《安全事件报告和处置管理程序》：明确安全事件的类型，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；确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；为造成系统中断和造成信息泄密的安全事件制定不同的处理程序和报告程序；

4)制定《安全事件等级划分方法》：根据国家相关管理科室对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分。

1.2.5.5.13 应急预案管理

制定《应急预案管理制度》：

1)指定责任科室：由信息中心负责应急预案管理；

2)建立统一的应急预案框架，框架应包括事件分级方法、各级事件启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

3)在应急预案框架制定不同事件的应急预案，应急预案要指名适用的系统、设备等，要结合系统实际状况，如《门户网站被篡改应急预案》、《网络设备瘫痪应急预案》；

4)资源承诺：从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

5)培训要求：对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

6)演练要求：定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；

7)更新要求：规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

1.2.5.5.14 外包运维管理

1)确保外包运维服务商的选择符合国家的有关规定；

2)与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；

3)保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；

4)在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

1.2.6 安全运维服务设计

本项目免费运维期内的安全运维服务由项目承建商免费提供，免费运维期满后的安全运维服务由运维服务商提供。

1.2.6.1 安全咨询服务

安全管理咨询

建议由专业的安全服务机构对重要业务系统进行全面的安全管理体系建设咨询。参考国内外相关标准和国内的安全规范要求，根据业务特点，协助管理部门进行安全管理组织、安全管理职责、安全管理策略、安全管理制度、安全管理流程等的制定和优化（对已有策略），帮助推动安全管理制度的有效落地，为网络安全管理和运维提供更好的指导和支持，确保网络安全管理正规有序。

应急预案咨询

建议由专业的安全服务机构协助贵州省无线电管理信息系统制定针对各类重大安全事件的安全应急预案。预案制定以后，还要针对预案内容进行必要的培训和操作性演练。通过培训和演练，培养贵州省无线电管理信息系统自身的应急队伍，使其熟悉应急工作流程，识别应急所需资源要求，评价应急准备状态，检验应急预案的可行性和改进预案，从而提高警惕性和实战能力。

代码安全咨询

建议采用专业安全服务机构提供的代码安全检查服务，在应用软件开发初期，通过使用

自动化的源代码检查工具结合安全专家的人工检查手段，识别应用软件安全问题，如不当的加密算法和可能导致漏洞的常见语义语言结构等，并根据行业安全规范要求和业界最佳实践指南为其他业务系统的安全开发规范，指导开发人员进行安全编程。

定期安全通告

对于网络管理人员，特别是复杂网络的管理人员，由于时间和工作关系，通常会遇到无法收集并分类相关的安全报告，使得网络中总或多或少的存在被忽视的安全漏洞。

通过服务的平台与客户及时交流，帮助客户保持领先的安全理念和技术。安全通告服务不是单一的、随处可见的邮件列表，而是针对实际情况，专业服务人员分类、整理、归纳的安全信息。

安全通告服务以邮件、电话、走访等方式，将安全技术和安全信息及时传递给客户。内容包括：

紧急安全事件通告；

业界最新动态；

国际、国内以及行业安全政策及法律法规；

各种信息系统的漏洞信息；

安全产品评测信息等。

通过安全通告服务，用户可以迅速、准确地了解安全业界的新方向，包括安全事件的新特点和技术产品新动态。此外，也会提供相应地统计数据和分析报告。安全通告服务的目的是使用户能够在细节上进行安全预警，在宏观上把握安全趋势，合理规划相应的安全工作。

凭借国内领先的安全研究能力，广泛的信息采集途径，以及和全球领先的漏洞信息收集系统，使得我们能高质量，高效率的完成这些整理、分析、测试、分类等工作。将最新最全面的网络安全问题以最快的速度通报给客户，并且给出相应的解决办法，从而大大减轻网管人员做安全技术追踪和分析的压力。

安全培训教育

技术培训主要是提高员工的安全意识和安全技能，使之能够符合相关信息安全工作岗位的能力要求，全面提高客户整体的信息安全水平。

针对不同层次的员工，进行有关信息安全管理的理论培训、安全管理制度教育、安全防范意识宣传和专门安全技术训练，确保组织信息安全策略、规章制度和技术规范的顺利执行，从而最大限度地降低和消除安全风险。

安全意识培训

通过对客户全体员工的安全培训和教育工作，提高全体工作人员的信息安全意识和操作水平，降低由于人为原因引发的安全风险。

技术类培训

针对具体负责网络安全运维的技术人员，进行系统化的专业培训，培训内容包括基础理论、技术原理，以及产品的功能、安装、配置及运行维护等方面的详细培训，并结合实验室上机试验，使参加培训的人员能够熟练的掌握产品的运行维护方法，能够独立管理和维护设备，同时对安全技术有较全面的了解。

管理类培训

针对客户不同层面、不同职责、不同岗位的人员进行培训，在客户方内部推行、实施已建立的安全管理体系，提高信息安全管理水平。

安全流程制度培训

针对相关的安全流程、安全制度、安全规范、安全运维计划进行培训，使员工了解相关的、系统级的安全体系操作流程和制度。

1.2.6.2 安全评估服务

网络设备评估

根据信息系统中设备类型的不同，对核心层、交换层和接入层及防火墙、入侵检测等边界网络安全设备的访问控制和安全策略，现状有针对性进行风险评估。

操作系统评估

网络服务器及可互联终端的安全始终是信息系统安全的一个重要方面，攻击者往往通过控制它们来破坏系统和信息，或扩大已有的破坏。

网络攻击的成功与否取决于三个因素：攻击者的能力；攻击者的动机；攻击者的机会。正常情况下，我们是无法削弱攻击者的能力和动机这两个因素，但有一点我们可以做到减少他们的攻击机会。

对操作系统开放的服务、安全配置、访问控制、系统漏洞进行安全脆弱性风险评估。

应用程序评估

应用程序本身存在一定的安全缺陷和隐患，攻击者可以利用应用程序中的漏洞入侵系统、窃取信息及中断系统服务。为保证客户重要业务系统保密性、可用性，对操作系统上基于WEB 服务及第三方应用程序做安全评估。

1.2.6.3 安全加固服务

由于功能复杂，代码庞大，计算机操作系统、数据库系统在设计上存在一些安全漏洞和

一些未知的“后门”，一般情况下很难发现，同时由于系统的配置不当也会带来安全隐患，是黑客攻击得手的关键因素。因此，信息系统在投入使用前和使用中，都需要对操作系统、数据库系统等进行安全加固，以提高系统安全防范能力，减少安全事件的发生。

安全加固是配置软件系统的过程，针对服务器操作系统、网络设备、数据库及应用中间件等软件系统，通过打补丁、强化帐号安全、加固服务、修改安全配置、优化访问控制策略、增加安全机制等方法，堵塞漏洞及“后门”，合理进行安全性加强，提高其健壮性和安全性，增加攻击者入侵的难度，软件系统安全防范水平得到大幅提升。

1.2.6.4 渗透测试服务

渗透测试，是一种从攻击者的角度来对主机系统的安全程度进行安全评估的手段，在对现有信息系统不造成损害的前提下，模拟入侵者对指定系统进行攻击测试。通过渗透测试，可以对用户信息平台的安全性得到较深刻的认知，可以用于验证经过安全保护后的系统是否真实的达到了预定安全目标。

渗透测试服务包含贵州省无线电管理信息系统中开放的操作系统、应用服务、网络设备的安全弱点分析，使用模拟黑客攻击的手段，对信息系统的各类安全弱点进行全方位的刺探，得出信息系统的技术脆弱性和被黑客攻击的可能性，并生成相应的渗透测试弱点报告以及解决建议报告。帮助客户认识和精确分析当前网络和信息系统中的安全风险现状，通过评估准确分析出目标系统对象上存在的安全隐患和安全漏洞。针对安全漏洞现状分析和编写安全漏洞统计报告和明细报告，根据漏洞分布情况提出当前目标针对性地安全解决方案和解决建议，从最深的技术层面发掘系统漏洞，提升整个系统的安全性，防患于未然，使黑客和恶意攻击者无懈可击。

1.2.6.5 安全配置检查服务

收集贵州省无线电管理信息系统业务系统及各关键设备和主机操作系统的安全补丁，检查各主机的系统和业务补丁加载情况，以及关键设备上的安全策略配置情况，并结合对关键设备和主机进行漏洞扫描、入侵渗透测试，根据扫描或渗透结果划分高、中、低风险提交安全加固方案和加固计划，并对加固效果进行评估，有效降低高危漏洞，提高主机及操作系统安全性。

安全配置检查服务将参照行业安全检查规范，根据贵州省无线电管理信息系统建设内容，适当的补充安全基线检查内容，使用软件自动及手工的方式对贵州省无线电管理信息系统中操作系统、中间件、数据库及业务应用系统进行全面检查及抽样检查，并输出报告。

1.2.6.6 应急响应服务

紧急事件响应，是当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。

紧急事件主要包括：

病毒和蠕虫事件

黑客入侵事件

误操作或设备故障事件

但通常在事件爆发的初始很难界定具体是什么。所以，通常又通过安全威胁事件的影响程度来分类：

单点损害：只造成独立个体的不可用，安全威胁事件影响弱。

局部损害：造成某一系统或一个局部网络不可使用，安全威胁事件影响较高。

整体损害：造成整个网络系统的不可使用，安全威胁事件影响高。

当入侵或者破坏发生时，对应的处理方法主要的原则是首先保护或恢复计算机、网络服务的正常工作；然后再对入侵者进行追查。因此对于客户紧急事件响应服务主要包括准备、识别事件（判定安全事件类型）、抑制（缩小事件的影响范围）、解决问题、恢复以及后续跟踪。

准备工作：

建立客户事件档案

与客户就故障级别进行定义

准备安全事件紧急响应服务相关资源

为一个突发事件的处理取得管理方面支持

组建事件处理队伍

提供易实现的初步报告

制定一个紧急后备方案

随时与管理员保持联系

识别事件

在指定时间内指派安全服务小组去负责此事件

事件抄送专家小组

初步评估，确定事件来源

注意保护可追查的线索，诸如立即对日志、数据进行备份（应该保存在磁带上或其它不联机存储设备）

联系客户系统的相关服务商厂商

缩小事件的影响范围

确定系统继续运行的风险如何，决定是否关闭系统及其它措施

客户相关工作人员与本公司相关工作人员保持联系、协商

根据需求制定相应的应急措施

解决问题

事件的起因分析

事后取证追查

后门检查

漏洞分析

提供解决方案

结果提交专家小组审核

后续工作

检查是不是所有的服务都已经恢复

攻击者所利用的漏洞是否已经解决

其发生的原因是否已经处理

保险措施，法律声明/手续是否已经归档

应急响应步骤是否需要修改

生成紧急响应报告

拟定一份事件记录和跟踪报告

事件合并/录入专家信息知识库

1.2.6.7 系统上线前检测服务

系统上线前检测是应用系统生命周期中的一个重要环节，在对应用系统建设规划和现状充分调研的基础上，制订系统上线前的安全检测方案，并根据信息系统平台建设情况，按照系统上线前安全检测方案实施检测工作，进行彻底全面的安全弱点评估，发现潜在的安全漏洞。上线前检测需采用对系统非侵害的测试方法，检验系统的安全防护能力，发现安全风险及漏洞，采用方法至少包括远程渗透测试、设计文档检查等。

通过上线前的检测工作，对应用系统所覆盖的全部资产再次进行确认识别，完成对应用系统等级保护建设措施落实情况的合规性分析，对应用系统等级保护实施的各项安全措施和管理制度进行全面的风险评估，明确残余风险；依据风险评估结果、上线前检测结果、合规

性分析结果，进行差距分析，提出安全改进建议。

六、贵州省无线电管理信息系统网络安全建设项目（主中心节点）设备数量及技术参数要求（招标限价 215 万元）

序号	设备名称	主要指标	数量	单位
一	网络设备			
（一）	核心交换域			
1	核心交换机	1、三层以太网交换机，≥4U 机架式设备，双主控，双电源，≥24 千兆电口，≥24 千兆光口，≥8 万兆光口，业务板插槽≥3； 2、交换容量≥20.8Tbps，IPv4 包转发率≥2880Mpps，包含 3 年硬件质保服务。	2	台
（二）	核心业务域			
1	汇聚交换机	1、交换容量≥2.56Tbps， 转发率≥220Mpps，MAC 地址表≥32K，路由表容量≥16K，ARP≥16K； 2、接口：≥8 千兆电+14 万兆光口； 3、支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准； 4、支持最大 9 台设备虚拟化；最大堆叠带宽≥160G； 5、支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换，支持多控制器（EQUAL 模式、主备模式）； 6、支持 IPv4 静态路由、RIP V1/V2、OSPF、BGP、ISIS；支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+，支持 IPv4 和 IPv6 环境下的策略路由； 7、支持 VRRPv2/v3（虚拟路由冗余协议）；支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 200ms。	2	台
2	超融合软件	性能要求：配置 6 颗 CPU 超融合软件授权，包含管理平台、计算虚拟化、网络虚拟化、存储虚拟化等虚拟化软件。 功能要求：一、云管理平台软件 1、超融合管理系统云管平台软件属于自主研发产品，拥有自主知识产权；管理系统可部署虚拟安全产品，采用完全分布式架构构建，包括计算、存储、网络及云管； ★2、对退役服务器的数据自动迁移至其它正常服务器节点；超融合管理系统可部署虚拟安全产品（包括分布式防火墙、下一代防火墙、WAF、负载均衡、数据库审计、VPN、堡垒机、基线核查、日志审计、终端杀毒等）采用具有自主知识产权产品，非使用第三方 OEM 产品，保证良好的兼容性和扩展性； 3、支持一键大屏显示功能，方便监控集群状态，展示内容包括集群整体拓扑展示、健康状态、资源统计、资源负载情况及	1	套

		告警信息，CPU、内存、存储及网络使用率可以通过 TOP5 方式进行展示； 4、支持基于 Web 界面快速扩容计算和存储节点，通过扫描主机或者手动添加的方式增加主机，扩大集群功能，支持基于界面自定义物理主机角色，角色包括计算角色、数据角色、接入角色； 5、支持自动化任务功能配置，可以自定义任务类型及执行策略，任务类型包括卷备份和集群巡检等，提升管理效率。 二、服务器虚拟化 1、支持主机高可用性功能（HA），当集群中的服务器节点发生故障时，该主机上的虚拟机可以自动在集群内的其它物理机上恢复运行； 2、支持虚拟机计算资源自动扩展功能，根据计算资源负载情况实现 CPU 和内存的自动扩展，无需人工干预，提升效率；支持虚拟机级别副本设置，可以按照业务的安全需求给不同虚拟机设置不同数量副本，提升灵活性； 3、支持通过 VNC 和 Spice 两种方式远程访问虚拟机控制台，支持 Spice 方式设置独立访问密码，保证访问安全性； 4、支持虚拟机最后一屏功能，指在发生意外故障导致的虚拟机停机，可以将虚拟机最后一屏信息进行截图，为后续排错提供依据； 5、支持 CPU 基准配置，实现同一集群内的异构 CPU 配置，集群中虚拟机可以在不同配置 CPU 的服务器上实现在线的迁移，提供更高的兼容性。 三、存储虚拟化 1、采用分布式的软件定义存储架构，且分布式存储属于自主研发产品，具有自主知识产权，不能使用开源分布式存储或基于开源分布式存储（如 Glusterfs、Ceph 等）二次开发的产品； 2、支持集群服务器节点数量、服务器磁盘在线扩容，支持磁盘退役功能，被设置为退役的硬盘，数据自动迁移到集群其它服务器节点磁盘中； 3、支持 2 个或以上多副本冗余技术实现数据高可用性；分布式存储通过多副本冗余技术实现数据高可用性，支持基于存储卷级别的副本设定，可以针对不同场景灵活配置不同级别的副本数，最小支持 1 副本，最高支持 6 个副本，副本实现跨磁盘、跨节点、跨机架放置模式； 4、超融合不仅支持文件存储、块存储，还应同时支持对象存储服务，可以向外部系统提供对象存储服务，支持 S3 及 Swift 接口类型，支持 SSL 加密传输，满足非结构化数据存储需求，减少存储额外开支；同时支持存储的 QoS 设置。 四、网络虚拟化 1、支持链路聚合满足网络故障切换和负载均衡能力；支持本地网络功能，通过划分不同的虚拟网络交换机和虚拟端口组进行网络规划，支持端口镜像功能；		

		2、支持实时监控业务可用性，对网络进行监控分析，对指定网络进行流量、协议及端口监控；支持本地网络功能，通过划分不同的虚拟网络交换机和虚拟端口组进行网络规划，支持端口镜像功能； 3、支持网络监控与分析功能，可以对指定网络进行流量、协议及端口监控，支持规则定义、信息过滤等，提供完整流量分析功能； 4、支持链路探测功能，可自定义源端和目标端，支持网络 IP、端口等参数的检测，方便网络排错； 5、支持可视化网络功能，网络功能通过软件定义形成独立的网元，包括虚拟交换机、虚拟路由器及虚拟出口等，可以通过鼠标拖拽网元及连线的方式构建可视化网络，实现网络环境的快速化构建。 五、资质要求：为保障客户超融合平台稳定，要求制造商具备 CSA CS-CMMI5 云安全能力成熟度模型集成评估证书，ITSS 云服务能力符合性评估 SaaS 服务资质，超融合软件拥有数据中心联盟颁发的超融合架构可信认证证书，超融合软件支持 IPv6 网络环境，拥有全球 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证。		
3	超融合硬件	CPU：2 颗处理器，主频不小于 2.0GHz，物理核数不小于 32 核； 内存：不小于 256GB DDR4； 固态硬盘：不小于 2 块 480GB 企业级固态硬盘； 固态缓存盘：不少于 1.92TB 固态缓存盘； 机械硬盘：不小于 40TB 企业级硬盘； 网卡：超融合集群单个硬件节点至少需要配置 4 个万兆网口以及 4 个千兆网口。	2	台
（三）	**其他**			
1	接入交换机	1、24*10/100/1000BASE-T 电口+4*1G/10G BASE-X SFP+端口； 2、交换容量≥672Gbps，IPv4 包转发率≥126Mpps，包含 3 年硬件质保服务； 3、支持 XModem/FTP/TFTP 加载升级，支持命令行接口（CLI），Telnet，Console 口进行配置，支持 RMON （Remote Monitoring）告警、事件、历史记录,支持电源的告警功能，风扇、温度告警，支持系统日志，分级告警，调试信息输出； 4、支持 GE 端口聚合,支持 10GE 端口聚合，支持静态，动态聚合，支持跨设备聚合； 5、支持 IEEE802.3x 流量控制（全双工），支持基于端口速率百分比的风暴抑制，支持基于 PPS 的风暴抑制，支持基于 bps 的风暴抑制； 6、支持 32k MAC 地址，支持黑洞 MAC 地址，支持设置端口 MAC 地址学习最大个数； 7、支持分布式设备管理，分布式链路聚合，分布式弹性路由，支持通过标准以太网接口等方式进行堆叠，支持本地堆叠和远	6	台

		程堆叠； 8、支持 L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP(IPv4/IPv6)地址、目的 IP(IPv4/IPv6)地址、TCP/UDP 端口号、VLAN 的流分类，支持入方向和出方向的双向 ACL 策略，支持报文重定向，支持灵活的队列调度算法,可以同时基于端口和队列进行设置,支持 SP、WRR、WFQ、SP+WRR 四种模式； 9、支持用户分级管理和口令保护，支持 802.1X 认证/集中式 MAC 地址认证，支持端口隔离，支持端口隔离，支持动态 ARP 检测，防止中间人攻击和 ARP 拒绝服务，支持 uRPF(单播反向路径检测)，杜绝 IP 源地址欺骗，防范病毒和攻击。		
二	安全设备			
（一）	网络接入域			
1	防火墙（核心产品）	性能要求：国产化 CPU，国产化操作系统，冗余电源，≥6 个千兆电口,≥4 千兆光口（含多模模块），≥2 个万兆光口（含多模模块）；整机吞吐量≥15G,应用层吞吐量≥12G,最大并发连接数≥400 万,新建连接数≥30 万。1 个接口扩展槽位，4T 机械硬盘；包含 3 年硬件质保服务，3 年攻击防护特征库升级。 功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数； 2、支持路由、交换、虚拟线、Listening、混合工作模式； 3、支持与本次项目配置的安全管理系统实现协同联动； 4、支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 5、★支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图证明材料并加盖原厂公章）； 6、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置,简化用户管理； 7、提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果； 8、支持 IPv4/IPv6 双栈工作模式,支持 RADVD、ND、RIPng、OSPFv3、BGP4+； 9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回； 10、支持对国产主流数据库应用、P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制，支持自定义应用特征； 11、支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；	2	台

		12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警； 13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御； 14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面； 15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤，如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等； 17、★产品具备信息安全产品自主原创证明证书。		
2	病毒过滤网关/防毒墙	性能要求：国产化 CPU，国产化操作系统，机械硬盘≥4T；≥6 个千兆电口（含 2 对 bypass），≥4 个千兆光口（含多模模块），4 万兆光口（含多模模块）,冗余电源,1 个扩展槽位,整机吞吐率≥15Gbps，最大并发连接数 800W，病毒检测吞吐率≥5Gbps；包含 3 年硬件质保服务，3 年特征库升级服务。 功能要求：1、★设备必须为专业的防病毒网关产品，非防火墙/下一代防火墙、UTM、IPS 等具有防病毒功能模块的产品（提供产品 web 管理主界面截图并加盖原厂公章） 2、支持双引擎双库，且两个引擎可同时工作，各个应用协议可分别选择使用不同的病毒扫描引擎（快速扫描引擎或深度扫描引擎）进行病毒检测； 3、能够防御病毒、木马、蠕虫、间谍软件等恶意软件，且支持对压缩数据、加壳病毒的检测与处理； 4、支持对 HTTP、FTP、POP3、 SMTP、IMAP 等常用应用协议进行病毒检测与过滤； 5、病毒引擎具备自动化的数据解压缩能力，无需手动配置，具备 64 层的数据解压缩病毒检测能力； 6、支持联动态势感知探针产品，识别未知病毒，防御 APT 攻击； 7、支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络，能够在该网络环境中检测出病毒流量； 8、流行病毒检测率不低于 95%，并提供国家专业病毒检测机构的证明； 9、病毒网关默认加载的流行病毒库总数大于 2000 万，可本地化完成病毒地检测过滤与处理，无需发送到云端检测； 10、支持 IP、ICMP、TCP、UDP、HTTP、HTTPS、SIP、NTP、DNS 等协议的 DDoS 攻击防御； 11、支持多条链路的即插即用病毒检测防御模式，可利用同一台病毒过滤网关实现多链路防护，增强业主单位网络安全性并节省业主单位的病毒防御成本；	2	台
（二）	**核心业务域**			

1	防火墙	性能要求：≥4T 机械硬盘；交流冗余电源；≥6 个千兆电口、≥4 个千兆光口、≥4 个万兆光口（满配万兆多模模块；支持 IPS、防病毒、应用控制、IPSec VPN、SSL VPN 等功能；网络吞吐≥40Gbps，应用吞吐≥32Gbps，最大并发连接≥1200 万，包含 3 年硬件质保服务，3 年攻击防护、病毒过滤特征库升级。 功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数； 2、支持路由、交换、虚拟线、Listening、混合工作模式； 3、支持与本次项目配置的安全管理系统实现协同联动。 4、支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 5、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； 6、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置,简化用户管理； 7、提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果； 8、支持 IPv4/IPv6 双栈工作模式,支持 RADVD、ND、RIPng、OSPFv3、BGP4+； 9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回； 10、支持对国产主流数据库应用、P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制，支持自定义应用特征； 11、支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； 12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警； 13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御； 14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面； 15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤，如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等；	2	台

2	Web 应用防护	性能要求：≥4 个 千兆电口、≥4 个千兆光口（含多模模块）、≥2 个万兆光口（含多模模块）； 32G 内存，4T 硬盘；冗余双电源；HTTP 吞吐：≥15Gbps； HTTP 新建（CPS）：≥120,000/s；HTTP 最大并发连接数：≥400 万；含网页防篡改功能，包含 3 年硬件质保服务，3 年特征库升级服务。 功能要求：1、支持无 IP 纯透明模式串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署。 2、支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口 3、支持对 HTTP 协议合法性进行验证，支持对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理； 4、支持针对主流 Web 服务器及插件的已知漏洞防护，Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等插件应覆盖:dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress 等，提供 Java 反序列化漏洞（Jboss）防护规则； 5、支持 HTTP 访问控制功能，可以提供针对 HTTP 元素和客户端的组合访问控制策略。支持对多种 HTTP 方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT； 6、扫描防护:攻击者通常会利用各种工具扫描网站，探测网站漏洞，给网站的安全带来极大隐患。WAF 可以通过识别扫描工具的数据特征值，阻断扫描工具的探测。支持基于请求量统计和应答分布统计等算法对扫描行为进行分析并防护； 7、人机识别:可通过 JS 脚本识别自动化工具，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测，识别攻击工具，主要包括市面上主流扫描器，如 burpsuite、nessus 等，市面上主流自动化工具 selenium、phantomjs 等的脚本攻击识别；	1	台
3	数据库审计	性能要求：≥6 个千兆电口，4 个千兆光口（含多模模块），≥2 个万兆光口（含多模模块），硬盘:2TB；1 个扩展槽;2 个 USB,1 个 CONSOLE 口;双电源；峰值入库速度:18000（条/秒）；无实例数限制，网络吞吐≥5G,SQL 吞吐≥1000M。默认 3 年硬件质保服务。 功能要求：1、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括常见操作系统、国产操作系统 2、支持细粒度解析数据库协议，包括关系型数据库、国产化数据库等。 3、支持 HTTP、Telnet、FTP、Rlogin 的审计 4、具备数据库操作类、表、视图、索引、触发器、游标、事	1	台

		务各种对象的 SQL 操作审计 5、支持数据库请求和返回的双向审计，特别是 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容 6、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。 7、支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估 8、支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示 9、支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，内置审计规则不需要额外配置，并进行实时报警； 10、支持以用户名、源 IP、部门、域名、主机名、邮箱、联系电话为条件的实名审 11、支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 语句、SQL 返回结果集、返回码、SQL 语句响应时间、SQL 操作类型、影响行数等条件的审计查询。 12、支持超长 SQL 语句审计，至少不低于 2M，支持多层嵌套 SQL 语句的审计，有效分割、准确审计主流数据库协议的多 SQL 语句		
（三）	**核心交换域**			
1	全威胁检测系统	性能要求：机械硬盘≥1TB，≥6 个千兆电口，≥4 个千兆光口（含多模模块），≥2 万兆光口（含多模模块），冗余电源,4 个扩展槽位,最大并发连接数：≥800W，综合威胁检测能力：≥10Gbps。含：3 年攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库升级许可。包含 3 年硬件质保服务 功能要求：1、★支持全流量取证，将事件发生前后的流量一起留存，支持攻击取证、僵尸主机取证、恶意程序样本、威胁情报取证，取证类型支持报文取证和样本文件取证两种形式。（（提供截图证明材料并加盖原厂公章）） 2、支持对设备进行网络参数配置，包括长连接占总连接的百分比、握手时 TCP 连接超时、TCP 超时时间、其他连接超时、TCP Reset、连接完整、只允许 SYN 报文建立新连接、长连接超时、关闭时 TCP 超时时间、UDP 超时时间、校验和检查、分片重组、快速连接重用等参数。 3、支持在线抓包，可配置抓包数量、协议类型、源 IP、源端口、目的 IP、目的端口、源或目的 IP、源或目的端口、文件	1	台

		名、接口、VLAN ID 等。支持在线多任务并行抓包 4、Syslog 支持配置多个服务器地址，支持 TCP、UDP 传输协议，支持 UTF8、GB2312 编码格式，支持选择是否以加密方式传输，可选择证书加密或密码加密。 5、支持独立的攻击检测引擎，支持 9700 种以上的攻击规则库。 6、支持能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、物联网漏洞攻击等在内的 16 大类超过 9700 种以上网络攻击事件，支持多种常见攻击行为进行检测。 7、支持自定义规则，并且自定义规则库可以导入导出。 8、★支持服务器非法外联检测，支持按 IP 地址、IP 范围、子网设置监测对象，支持仅对外联境外地址监测，支持按 IP 地址、IP 范围、子网设置外联白名单。支持对服务器外联行为自学习，自动记录外联信息，包括 IP 地址、协议、端口/ICMP 类型、连接数。（提供截图证明）可设置相应警告、联动阻断动作。（提供截图证明并加盖原厂公章） 9、支持独立的 DDoS 检测引擎，支持对 IP 扫描攻击、端口扫描攻击等多种扫描攻击行为检测； 10、支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响，可对检测到的恶意文件设置相应警告、联动阻断动作；支持专业沙箱设备联动检测。 11、支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸行为规则库检测已知的 APT 组织。 12、支持对 SQL 注入攻击、跨站攻击、浏览器劫持攻击、URL 跳转攻击、WEB 远程代码执行攻击、WEB 缓冲区溢出攻击、WEB 漏洞攻击、Webshell 上传攻击、WEB 越权攻击、WEB 扫描攻击、目录遍历攻击、WEB 口令暴力破解攻击等多种类型的 WEB 攻击检测。 13、本地嵌入独立的威胁情报库，不依赖其他设备或情报平台，即可独立的实现威胁情报检测能力，可对检测到的恶意文件、恶意 IP/域名、恶意 URL 设置相应捕获、联动阻断动作。 14、支持卸载 SSL，实现对 HTTPS、IMAPS、SMTPS、POP3S、FTP、RDP、MQTT、SIP 等加密流量的分析检测。 15、支持数量超过 1000 万的 URL 分类库，URL 类型涉及包括搜索引擎、网上购物、社交网络、求职招聘、财经、下载、政策法规、成人内容、非法及不良等。		
（四）	**安全管理域**			
1	网络准入控制	性能要求：≥6 个千兆电口，终端授权支持扩容≥5000 点；本次项目配置≥400 点终端授权。三年硬件质保。 功能要求：1、支持双操作系统冷备、双机热备，在单机模式下，提供独立系统逃生工具。	1	台

		2、支持策略路由、端口镜像、透明网桥、802.1X、ARP、DHCP、VLAN 隔离、Portal 等准入技术，支持准入技术自由组合使用，满足各种复杂网络环境； 3、支持划定关键业务范围，针对终端用户发起的访问请求可强制要求二次认证校验； 4、能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP 表等信息；支持在界面上提供对该网络设备进行 TELNET、SSH 等管理；能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接； 5、支持设置来宾专属地址段；来宾入网提供二维码、来宾码、自助申请（管理员审批）多种方式；提供来宾入网审批气泡弹窗提醒功能，被访人点击即可审批； 6、移动终端可以支持通过将指纹和用户账户绑定的方法，实现用户按压指纹认证入网； 7、软件、消息分发：支持基于部门、角色（分组）、设备或 ip 段进行软件、消息分发，分发周期支持立即、每天、每周、每月等周期设置。针对分发的源文件支持设置保留或不保留，分发后支持重启或关闭计算机； 8、在无客户端的方式下，可发现终端同时连接内网和外网的行为，在外网违规外联服务器上能够查看到违规外联条目信息；针对违规外联的终端能够阻断起内网连接；		
2	运维安全审计	性能要求：≥6 个千兆电口；≥2TB 硬盘，交流冗余电源；≥ 100 个资产管理授权；包含 3 年硬件质保服务，3 年特征库升级服务。 功能要求：1、支持物理旁路部署，不改变现有网络结构； 2、支持第三方证书用户自行上传用作校验的 CA 证书和 CRL 列表； 3、本地 CA 支持根证书的重新生成及替换；支持根据根证书签发出客户端证书；支持发布生成吊销列表；支持国密证书认证。 4、支持资源分类和资源系统类型管理：内置常见资源分类和资源系统类型，可自定义添加资源分类、资源系统类型和资源服务类型 5、支持对已添加的设备账号进行密码托管，从而实现单点登录功能； 6、自动对数据库、Windows、Linux 等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成； 7、支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权； 8、支持会话、指令、剪切板上下行、文件上传下载的约束行为； 9、提供授权关系查看功能，图形化直观展示用户、资产、协	1	台

		议、账号的授权关系 10、支持会话请求远程协助，且协同会话保持实时同步； 7、11、支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。 12、支持自动执行运维脚本。运维脚本分为内置和自定义。 13、支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现 IT 资源的动态分配、灵活调度、跨域共享，提高 IT 资源利用率。 14、支持配置数据和审计数据的备份、自动清理，支持备份数据通过 FTP 方式远程备份；支持磁盘映射手动/自动清理；		
3	日志审计	性能要求：存储空间≥6T 硬盘，32G 内存，≥4 个千兆电口，4 个千兆光口（含多模模块），冗余电源；≥8000EPS，200 个管理设备授权；出厂默认 3 年软硬件质保服务。 功能要求：2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。 3、对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可； 4、支持主动、被动相结合的数据采集方式；支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。 5、系统内置已支持设备种类清单，提供设备日志外发配置建议指导 6、支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； 7、支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； 8、支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集； 9、支持根据设备重要程度独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数； 10、支持原始日志全文检索； 11、支持在一个日志源查询结果列表中将 IP 作为源地址或目的地址查询条件，直接跳转到其他日志源类型中进行查询； 12、系统内置安全知识库，支持自定义增加安全知识内容，可在关联分析规则中关联知识。	1	台
4	态势感知平台（核心产品）	性能要求：≥6 个千兆电口，≥2 个万兆光口（含多模模块），冗余电源,1 个扩展槽位,双 CPU，≥256G 内存，≥40TB 硬盘，支持 raid，数据采集器性能≥20000 条/秒；支持 10 亿条数据秒级检索响应。 支持态势监测、响应处置、分析研判、资产管	1	台

		理、集中管控、安全治理、安全审计、威胁情报等功能模块。配置 20 个联动设备接入授权,3 年质保，3 年系统升级服务 功能要求：★1、 提供全网态势、威胁态势、资产态势、漏洞态势、攻击态势、恶意程序态势等展示界面（提供截图证明材料并加盖原厂公章） 2、支持安全处置功能：支持告警工单处置人、告警处置结果、未处置状态统计及详情。 3、支持漏洞监测功能： 支持联动漏扫设备或手动导入漏扫报告方式实现漏洞数据采集，支持不同品牌漏扫设备联动，支持 excel、zip 等类型的漏扫报告导入； 4、支持响应编排功能：支持基于场景的安全策略响应编排 5、支持工单管理功能，支持指派相关责任人进行处理，支持对工单进行分组管理，分组类型包括我的工单、待处置工单、已处置工单、历史工单： 6、支持资产管理功能：支持资产新增、修改、删除，支持自定义资产信息，包括资产三性等基本信息、资产类型、所属业务系统、所属物理位置、责任人、漏洞、补丁及软硬件信息等，支持资产批量删除、资产导出、资产导入 7、支持管控设备概览功能：支持通过界面快速添加集中管控设备， ★8、支持管控设备拓扑图展示功能：支持拓扑动态提示管理设备产生的告警，支持拓扑图右击直接查看选中设备的设备概览、设备详情、告警列表等信息，支持设备策略集中管理功能：包括配置信息、运行配置、配置备份、模块管理、日志外发、升级管理、配置审计，支持日志外发地址、端口、协议配置，支持设备升级的版本号、序列号展示，支持设备操作记录审计，包括审计时间、配置类型、结果状态、执行设备地址、执行设备名称、执行设备类型、操作人、审计内容等（提供截图证明材料并加盖原厂公章） 9、支持设备策略集中管理功能：包括配置信息、运行配置、配置备份、模块管理、日志外发、升级管理、配置审计，支持日志外发地址、端口、协议配置，支持设备升级的版本号、序列号展示，支持设备操作记录审计，包括审计时间、配置类型、结果状态、执行设备地址、执行设备名称、执行设备类型、操作人、审计内容等。 10、支持全网策略概览功能：支持下发策略统计、配置备份统计、活跃策略、最新下发策略操作人、最新下发策略设备、最新策略任务、最新配置备份、最新失败审计等监控能力 11、支持多种类型设备策略配置功能：支持多种策略配置，包括但不限于访问控制策略、静态黑名单、动态黑名单、安全策略等 12、支持全部被管设备配置集中审计，支持审计查询， 13、支持安全报告功能：包括但不限于安全报告、合规审计日志、应急预案、跟踪文档、待整改业务系统展示，支持待整改		

		业务系统排名、最新安全报告排名、最新跟踪文档等信息，最新安全报告支持下载 14、支持应急预案：包括但不限于可疑异常、设备故障、网络攻击、内容安全、有害程序、信息破坏分类； 15、支持内生情报管理功能：包括恶意 IP 地址、恶意 URL、恶意样本、恶意域名、垃圾邮件等，支持情报进行分类自定义查询，支持自定义威胁情报信息，支持威胁情报的导入		
5	无线电管理平台防护系统(核心产品)	1、配置 1 套无线电管理平台防护系统，实现对无线电管理一体化平台的两个集群进行防护安全防护。3 年升级服务 功能要求：1、采用 Agent-Server 架构，支持通过 B/S 管理方式对主机进行集中管理。 2、Agent 运行支持业务优先、均衡模式、防护优先等运行模式，以应满足不同应用场景。 3、支持通过管理端对 agent 进行批量启用、停用、卸载、删除、升级和重连，支持按 agent 版本、操作系统版本、agent 状态、在线状态、安装时间等进行搜索。 4、★采用 ARP、PING 扫描、NMAP 扫描多种探查方法，主动发现未安装安全探针的主机的信息，包含 IP 地址、MAC 地址、操作系统、安装状况、最近扫描方式等，支持以模板 xlsx 格式手动导入资产。（提供 CNAS/CMA 资质的第三方测试报告） 5、★支持扫描中间件漏洞，包括但不限于 Apache、Nginx、Tomcat，可以扫描 SQL 注入、XSS 跨站点脚本、命令行注入、CSP 配置漏洞、目录遍历攻击等网站漏洞，支持查看风险详情，提供修复建议，支持对操作系统及 MySQL、Redis 等应用的弱密码进行检测，支持字典管理等功能；（提供截图证明材料并加盖原厂公章） 6、支持实时检测内核后门、引导后门、勒索病毒、流氓程序、黑客工具等病毒，检测内容至少包含类型、病毒名称、病毒 ID 等信息，支持隔离、信任、删除、溯源操作。 7、支持检测 SSHD、FTP、RDP 等暴力破解入侵行为，灵活配置检测策略，包含设置攻击检测周期、攻击次数阈值与处理方式（包含仅记录和记录自动停封），提供白名单和黑名单。 8、支持实时检测异常 IP、异常区域、异常时间、异常账号等异常登录行为，展示威胁事件详情，包含主机 IP、登录区域、登录账号、来源、登录时间、异常类型等。 9、实时检测 ASP、ASPX、PHP、JSP 等 Webshell 后门，支持隔离、信任、删除、溯源操作。 10、实时检测隐藏进程、隐藏端口号进程、子权限大于父权限等异常进程并产生告警，包括异常进程、进程路径、进程 ID、父进程 ID、状态等，支持对异常进程加黑处理 11、实时检测提权行为并产生告警，告警信息至少包括被提权主机 IP 地址、发现时间、提权进程、提权用户、进程 ID、父进程 ID 等，支持设置黑名单。 12、实时监控系统命令篡改行为，防止命令注入攻击，告警信	1	套

		息包括篡改命令、主机 IP 地址、操作路径，支持设置白名单。 13、提供中标麒麟、银河麒麟、Suse、CentOS、RedHat、 Ubuntu 等操作系统基线模板；Apache、Nginx、Tomcat、Weblogic、Redis、MySQL、DB2 等应用基线，支持提供等保二级、三级主机安全合规检查基线，支持提供 CIS Level1、Level2 基线。		
6	漏扫	性能要求：1 个 CONSOLE 口，≥2 个 USB 口；≥6 个千兆电口，≥2 个千兆光口；1T 硬盘； 支持系统扫描，最大可扫描 IP 或域名数无限制，扫描任务并发 5，扫描 IP 并发 80； 支持 Web 扫描； 支持弱口令检测；包含 3 年硬件质保服务，3 年特征库升级服务。 功能要求：1、支持扫描主流操作系统、Web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞 2、支持 IPv4/IPv6 双协议栈地址场景漏洞扫描 3、支持防火墙联动功能，防火墙能根据漏扫提供的资产信息对重要资产信息进行防护，根据漏洞信息自动生成防护规则，保护内网安全； 4、支持外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，支持加密传输 5、支持扫描系统漏洞数量大于 240000 种，web 漏洞数量大于 5000 种,数据库大于 3000 种，CVE 漏洞数大于 60000； 6、产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号 7、支持扫描大数据组件的安全漏洞，如 Spark、Splunk、Kafka、Storm、Cassandra、Ambari、Impala、Solr、Oozie、Hbase、Hadoop 等 8、扫描目标支持 ip、域名、网段、子网的组合配置； 9、主机存活探测支持 ARP ping、ICMP ping、TCP ping、UDP ping、TCP SYN Ping、TCP ACK Ping 等多种方式 10、支持对 DB2、MSSQL、MySQL、Oracle、GBASE、DMDB 等主流数据库进行登陆认证扫描； 11、支持站点组、单站点风险在线报表和站点特有属性配置 12、支持排除路径名，可自定义无需爬取的 URL 链接； 13、支持主流操作系统配置核查， 包括但不限于 Windows、Linux、BClinux、 Solaris、HPUnix、AIX 等操作系统，支持中标麒麟、优麒麟、中兴新支点等国产化操作系统 14、支持 Elasticsearch、ZooKeeper、Spark、HDFS、Kafka、HBase、Hive、Sqoop、Yarn-MR、Impala 等大数据组件的配置核查	1	台

七、贵州省无线电管理信息系统网络安全建设项目（备份中心节点）设备数量及技术参数要求（招标限价 29 万元）

序号	设备名称	主要指标	数量	单位
一	网络设备			
1	核心交换机	1、标准配置：三层以太网交换机，≥4U 机架式设备，双主控，双电源，≥24 千兆电口，≥24 千兆光口，≥8 万兆光口； 2、交换容量≥20.8Tbps，IPv4 包转发率≥2880Mpps，包含 3 年硬件质保服务。	1	台
二	安全设备			
1	防火墙	性能要求：国产化 CPU，国产化操作系统，冗余电源，≥6 个千兆电口,≥4 千兆光口（含多模模块），≥2 个万兆光口（含多模模块）；整机吞吐量≥15G,应用层吞吐量≥12G,最大并发连接数≥400 万,新建连接数≥30 万。1 个接口扩展槽位，4T 机械硬盘；包含 3 年硬件质保服务，3 年攻击防护特征库升级。 功能要求：1、支持日志外发至多个 SYSLOG 服务器，可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数； 2、支持路由、交换、虚拟线、Listening、混合工作模式； 3、支持与本次项目配置的安全管理系统实现协同联动。 4、支持 IP/MAC 绑定，支持跨三层绑定，支持 IP/MAC 绑定表导入导出，以便对 IP/MAC 绑定关系进行批量操作； 5、支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； 6、支持一体化安全策略配置，可以通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、邮件安全、数据过滤、文件过滤、审计、APT 等功能配置,简化用户管理； 7、提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在 WEB 界面显示检测结果； 8、支持 IPv4/IPv6 双栈工作模式，支持 RADVD、ND、RIPng、OSPFv3、BGP4+； 9、支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回； 10、支持对国产主流数据库应用、P2P、移动应用、下载软件加密流量、远程控制软件、工控物联网协议进行识别控制，支持自定义应用特征； 11、支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； 12、支持行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；	1	台

		13、支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御； 14、支持自定义 URL 分类和地址，支持 URL 黑/白名单，支持自定义阻断页面； 15、支持文件过滤，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测 16、支持内容过滤，如 FTP 上传文件、下载文件、删除文件或文本、重命名、创建目录、删除目录、显示文件列表等；		
2	日志审计	性能要求：存储空间≥6T 硬盘，32G 内存，≥4 个千兆电口，4 个 SFP 插槽（含多模模块），冗余电源；8000EPS，200 个管理设备授权；出厂默认 3 年软硬件质保服务。 功能要求：2、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集。 3、对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可； 4、支持主动、被动相结合的数据采集方式；支持 Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。 5、系统内置已支持设备种类清单，提供设备日志外发配置建议指导 6、支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；（ 7、支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； 8、支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集； 9、支持根据设备重要程度独立设置每个被采集源的日志、报表数据存储时间为 1 个月、3 个月、6 个月和永久保存等参数； 10、支持原始日志全文检索； 11、支持在一个日志源查询结果列表中将 IP 作为源地址或目的地址查询条件，直接跳转到其他日志源类型中进行查询； 12、系统内置安全知识库，支持自定义增加安全知识内容，可在关联分析规则中关联知识。	1	台
3	数据库审计	性能要求：≥6 个千兆电口，4 个千兆光口（含多模模块），≥2 个万兆光口（含多模模块），硬盘:2TB；1 个扩展槽;2 个 USB,1 个 CONSOLE 口;双电源；峰值入库速度:18000（条/秒）;无实例数限制，网络吞吐≥5G,SQL 吞吐≥1000M。3 年硬件质保服务。 功能要求：1、对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，适配的操作系统至少包括常见操作系统、国产操作系统 2、支持细粒度解析数据库协议，包括关系型数据库、国产化数据	1	台

		库等。 3、支持 HTTP、Telnet、FTP、Rlogin 的审计 4、具备数据库操作类、表、视图、索引、触发器、游标、事务各种对象的 SQL 操作审计 5、支持数据库请求和返回的双向审计，特别是 SQL 返回结果集、SQL 语句响应时间、连接时长、表影响的字段、影响行数等内容 6、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。 7、支持依据数据库实例监控各个数据库的连接池、缓冲区、表空间、死锁、CPU、内存、硬盘等信息，可自定义告警阈值进行健康评估 8、支持数据库服务器弱口令扫描，扫描出的弱密码支持脱敏显示 9、支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为，利用漏洞攻击等行为进行审计，内置审计规则不需要额外配置，并进行实时报警； 10、支持以用户名、源 IP、部门、域名、主机名、邮箱、联系电话为条件的实名审计 11、支持基于数据库时间、源/目的 IP、数据库名、应用协议、数据库表名、字段值、预处理 SQL、SQL 语句、SQL 返回结果集、返回码、SQL 语句响应时间、SQL 操作类型、影响行数等条件的审计查询。 12、支持超长 SQL 语句审计，至少不低于 2M，支持多层嵌套 SQL 语句的审计，有效分割、准确审计主流数据库协议的多 SQL 语句。		

八、其他要求

1、中标人需完成本项目中所包含软硬件设备的安装、本机调试、联网调试等集成服务内容（**集成费招标限价 20 万元**）。

2、主中心节点设备、备份中心节点设备、集成费用须分别报价。

3、中标人需配合完成针对贵州省无线电管理信息系统网络安全建设项目的等保测评，并根据测评结果完成整改直至通过等保测评。

第二节 商务要求

(一)基本要求

1.本招标项目的所有货物交货时的拆箱、安装、调试等工作由中标人负责，但必须在建设单位、监理单位参与下进行。

2.投标人必须保证提供的货物是原装全新(包括零部件)。

3.项目实施过程中应严格按照国家相关规范执行，若出现安全问题由中标人全权负责。

4.项目涉及的设备所产生的拆除、运输等一切费用由中标人承担。

5.人员要求：投标人应根据项目范围与工作需求，合理配置不少于5名具有相关项目经验的人员开展相关工作。

(二)项目服务期及地点

1.项目建设周期：

(1)在合同签定后待收到甲方开工令之日起90个日历天安装完成且调试验收合格。

(2)通过合同验收后实施系统试运行，试运行时应该满足全部的软件功能和性能要求。试运行时间为1个月。在试运行期间，出现非采购人因素导致的严重系统故障的，试运行期顺延，重新按1个月计算。试运行期正常结束后，可进行项目初步验收。

试运行期间系统正常运行主要是指：

①设备系统的运行稳定、可靠，未出现严重系统故障；

②系统的性能和功能满足采购人的要求。

如在合同约定时间内由于中标人的原因不能完成安装调试和部署，中标人应承担由此给采购人造成的损失。

2.交货地点：采购人指定地点。

(三)付款方式

合同签订后30个日历日内，采购人支付合同金额的40%作为预付款；项目合同验收合格后30个日历日内，采购人支付合同金额的50%（支付前，中标人须提供银行出具的与预付款等额的预付款保函，保函期限为1年）；项目初步验

收合格后30个日历日内，采购人支付合同金额的10%；中标人完成竣工验收后，采购人按规定办理银行保函退还相关手续。

(四)履约保证金

中标人在签订合同前，须以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式向采购人交纳中标金额10%的履约保证金；签订合同后，若中标人不按双方签订合同规定履约，则无权要求退回履约保证金。履约保证金不足以赔偿损失的，按实际损失赔偿；履约保证金在项目竣工验收合格后无息退还。

(五)验收方式

中标人根据项目实施进度情况提出验收申请，验收包括合同验收、初步验收和竣工验收等环节，都通过后方可完成验收，验收有关的费用均包括在投标总价中。验收时中标人须提供(但不限于)需求分析报告、项目实施方案、项目配置清单、系统功能测试报告、试运行报告、用户操作手册、培训记录，包含在系统内的第三方产品的随机资料等。

1.合同验收：

(1)核心设备到货后由双方共同开箱检验，根据合同清单开展货物（品名、型号、数量等）核验校对工作，采购人根据需要抽测货物技术指标是否符合技术要求，中标人按合同约定完成相关各类文档的收集，向采购人提请合同验收。

(2)合同验收合格后项目进入试运行，试运行不少于1个月。

2.初步验收：依据项目设计文件、招投标文件和合同，完成项目安装部署，并经试运行满足招标文件和合同要求,能够满足使用要求,完成档案材料的收集、整理，达到验收标准。

3.竣工验收：初步验收完成后，中标人配合采购方完成项目所有资料整理，并完成竣工验收。

(六)质量保证及售后服务

1.质量保证期

(1)投标产品质保期为自竣工验收合格之日起，质保期3年，中标人在质保期期间免费提供保修、运维及升级服务，有更优惠的质保请在投标文件中列明。

(2)投标产品由制造商(指产品生产制造商，或其负责销售、售后服务机构，

以下同)负责标准售后服务的，应当在投标文件中予以明确说明。

2.售后服务内容

(1)技术支持和服务

①电话咨询

中标人应当为采购方提供技术援助电话，解答采购方在使用中遇到的问题，及时为采购方提出解决问题的建议。针对信息系统，电话咨询服务需覆盖系统功能操作、数据查询、权限设置等常见使用问题解答。

②技术升级

在质保期内，如果中标人和制造商的产品技术升级，中标人应及时通知采购方，如采购方有相应要求，中标人应对采购方购买的产品进行免费升级服务。对于信息系统，中标人需提供升级前的功能兼容性测试报告，升级过程中需做好数据备份与恢复预案，升级完成后需进行系统功能与性能的全面测试，并向采购方提交测试报告。

③故障响应时间要求

质保期内出现质量问题，中标人在接到通知后24小时内响应到场，48小时内完成维修或更换，并承担维修调换的费用;采购方有权退货并追究中标人的违约责任。货到现场后由于采购方使用不当造成的问题，中标人亦应负责修复，费用由采购方负担。对于信息系统故障，中标人除到场处理外，需在接到通知后2小时内提供远程应急解决方案，若远程无法解决再进行现场处理。涉及数据丢失或系统崩溃等重大故障，需在48小时内恢复系统正常运行，并提供故障原因分析及预防措施报告。

④系统优化

中标人根据业务运行情况、网络情况对平台的系统参数提供优化建议，确保系统随着业务的发展能够持续、稳定、高效地运行。当系统功能扩充或系统性能下降时，中标人须主动或根据采购人要求，分析系统现状，在深入了解采购人目前及未来几年内的需求后,对硬件扩容和改造、软件平台改造提出合理化建议，并及时提供实施方案。此外,中标人需每月对信息系统进行一次全面的巡检工作，确保机房运行正常。

注：投标人按上述要求如实提供相关证明材料，如未按要求提供或提供资料不全，则与之相关的评分项不予计分。投标人提供的证明材料必须清晰有效，如因材料模糊不清评审小组无法辨认导致不得分的，其责任由投标人自行承担

第六章　合同条款

第一节　拟签订的政府采购合同

政府采购
(货物类)

甲方：（采购人全称）

乙方：（供应商全称）

甲、乙双方根据　项目名称　项目（交易编号：2015-ZFCG-XXXX,）的（采购方式）结果，甲方接受乙方为本项目的供应商。甲乙双方根据本项目采购文件、投标文件及招投标过程中确定的有关内容，签署本合同。

一、采购清单

1.1 货物清单

序号	采购货物名称	单位	数量	规格型号、技术参数
1				
2				
3				
……				

1.2 质量标准：须达到国家规定标准。

二、合同金额

2.1 本合同金额为（大写）：元（￥元）人民币。

2.2 本项目合同金额为本项目招标范围内所有货物服务的总价包干价。

三、技术资料、协调

3.1 甲方向乙方提供货物安装的有关技术资料。

3.2 甲方应配合乙方全力协调安装过程中所涉及的各部门工作，在协调过程中所耽误时间不计入乙方工期。

3.3 乙方应按采购文件规定的时间向甲方提供使用货物的相关技术资料及安装进度计划安排。

3.4 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的专利权、商标权或著作权等。

五、无产权瑕疵条款

5.1 乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。如乙方所交货物有产权瑕疵的，视为乙方违约，按照本合同第 13 条第 3 款的约定处理。但在已经全部支付完货款后才发现有产权瑕疵的，除了支付违约金，乙方还应负担由此而产生的一切损失。

六、质保期和质保金

6.1 质保期个月（自本项目安装验收合格之日起计）

6.2 如质保期内乙方提供的货物经验收无质量问题，待质保期满后由 甲方 接到乙方申请退付意见书后在五个工作日内无息退还。

七、供货安装期：按投标承诺期。

八、货款支付

8.1 付款方式：在签订合同后货物运送到达并支付合同总价款，待安装调试能正常使用天后支付合同总价款的，剩余 部分作为质保金，该质保金在正常使用天后无任何质量问题将全额无息返还。中标人所供货物运到采购人指定地点后，由采购人组织有关部门对其货物进行验收，验收合格后方可付款。

8.2 当本项目招标货物数量超出招标范围时，根据采购人实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价（投标文件中分项报价表中所列单价）进行计算。

8.3 招标过程中，如采购人、供应商或采购代理机构存在违法行为，在相关管理部门调查期间、被行政处罚期间，管理部门可视情况书面通知采购人暂停招

标活动，采购人将延期支付货款。

九、质量保证及售后服务

9.1 乙方应按采购文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品并将货物安装调试完成，使甲方能很好的使用。

9.2 乙方提供的货物在质量期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

9.3 如在使用过程中发生质量问题，乙方在接到甲方通知后在 12 小时内到达甲方现场。

9.4 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

9.5 上述的货物免费保修期为 12 个月，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

十、货物包装、发运及运输

10.1 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

10.2 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

10.3 乙方在货物发运手续办理完毕后24小时内或货到安装现场48小时前通知甲方，以准备验收货物。

10.4 货物在竣工验收合格前发生的风险均由乙方负责。

10.5 货物在规定的期限内由乙方安装完毕并通过甲方验收合格视为交付。

十一、调试和验收

11.1 甲方对乙方每个工程进度时间段需安装的货物依据采购文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合采购文件技术要求的，给予签证，初步验收不合格的不予签证。

11.2 乙方安装货物前应对产品作出全面检查和对验收文件进行整理，并列出

清单，作为甲方验收、签证和使用的技术条件依据，检验的结果交甲方。

11.3 乙方负责设备到货地点的安装调试，该安装调试应规范，乙方安装完毕需负责培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。培训所需一切费用均由乙方承担。

11.4 验收时甲乙双方、及相关单位必需在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。如果任何被检验的货物不能满足数量、规格、质量的要求，甲方可以拒绝接受货物，乙方应无条件更换被拒绝的货物，由此产生的损失由乙方承担。

十二、违约责任

12.1 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

12.2 甲方无故逾期验收和办理货款支付手续的，甲方应按逾期付款总额每日万分之五向乙方支付违约金。

12.3 乙方逾期交付验收合格的，乙方应按付款总额每日万分之五向甲方支付违约金，由甲方从待付货款中扣除。如因乙方原因造成工程逾期超过约定日期 10 个工作日不能交付竣工验收的，甲方可解除本合同。乙方因逾期交付验收或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值 5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

12.4 乙方所提供的货物品种、型号、规格、技术参数、质量不符合合同规定及采购文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

十三、不可抗力事件处理

13.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

13.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

13.3 不可抗力事件延续 30 天以上，双方应通过友好协商，确定是否继续履行合同。

十四、安全责任

在安装过程中的一切安全事故，由乙方自行负责，与甲方无任何关系。

十五、诉讼

15.1 双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向有管辖权的法院提起诉讼。

十六、合同生效及其它

16.1 合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

16.2 合同执行中涉及招标资金和招标内容修改或补充的，须经当地财政部门审批，并签订书面补充协议报监督管理部门备案，方可作为主合同不可分割的一部分。

16.3 下述合同附件为本合同不可分割的部分并与本合同具有同等效力：

（1）供货清单和分项价格表
（2）技术规格
（3）乙方报价函（及开标一览表）的内容及其澄清内容
（4）其他与本合同相关的资料
（5）本合同适用的特殊条款

16.4 本合同未尽事宜，遵照《合同法》有关条文执行。

16.5 本合同正本一式两份，具有同等法律效力，甲乙双方各执一份；副本三份，由采购人自合同签订之日起七个工作日内报监督管理部门备案。

甲方：

地址：

法定代表人：

授权委托代理人：

电话：

传真：

邮政编码：

乙方：

地址：

法定代表人：

授权委托代理人：

电话：

传真：

邮政编码：

开户银行：

账号：

签订地点：　　签订日期：　　年　月　日

注意事项：本合同条款未尽事宜，由甲乙双方以补充合同约定，原则上不能超越和违背招标及补充文件、投标文件及投标有关承诺的范围及内容。

（格式仅供参考）

投标文件格式

序号	文件夹/文件名称
1	响应文件封面
2	报价部分
2.1	投标函
2.2	报价明细表
3	整本响应文件

响应文件封面

【替换为项目名称】

响应文件

项目序列号: _____

项目名称: _____

标包名称: _____

标包编号: _____

供应商: _____

详细地址: _____

联系人: _____

电 话: _____

日 期: __年__月__日

投标函

1、我公司就【替换为项目名称】的【替换为标包名称】的 【投标报价名称】（元）为（大写）：____元人民币，小写：____元。【投标报价名称 1】(%)以折扣率形式进行报价为_____ %，【投标报价名称 2】（%）以下浮率形式进行报价为_____% 。

2、交付期（日历天）：_____

3、备注：_____

4、开标一览表内其他内容：_____

供应商名称（盖章）：_____

法定代表人或授权代表：____

地 址：_____

电 话：_____

传 真：_____

邮 编：_____

日 期：__年__月__日

投标文件格式范本

（响应文件封面格式）

_____项 目

响 应 文 件

采购项目名称：_____

采购项目编号：_____

投标单位名称：_____

地　　址：_____

联　系　人：_____

联 系 电 话：_____

响应文件目录

（格式自拟）

投 标 函

致：大成工程咨询有限公司

根据贵单位项目编号为 {项目编号} 的 {项目名称} 项目的投标邀请，（姓名）经正式授权并代表 供应商名称 提交响应文件。

据此函，签字代表宣布同意如下：

一、我公司的投标总价为（注明币种，并用文字和数字表示的投标总价）（必须按要求填写清楚）。

二、我公司将按磋商文件的规定履行合同责任和义务。

三、我公司已详细阅读了全部磋商文件，包括更正公告、澄清通知等（如果有的话）。我们完全理解并同意放弃对这方面有不明及误解的权力。

四、本投标有效期为磋商之日起 90 日历天。

五、如果在规定的投标截止期后，我公司在投标有效期内撤回投标，其投标保证金将被不予退还。

六、我公司同意并按照贵单位要求提供与投标有关的一切数据或资料，完全理解贵单位不一定接受最低价的投标或收到的投标，并承认贵单位有选择和拒绝任何供应商中标的权力（部分或全部设备）。

七、我公司承诺中标后，将按磋商文件规定的标准向贵方支付代理服务费。

投标供应商：_____（盖 章）_____

单位地址：_____

法定代表人或其授权委托人：_____（签字）_____

邮政编码：_____

电话：_____

法定代表人身份证明书（适用于法定代表人参加投标）

单位名称：_____

单位性质：_____

地　　址：_____

成立时间：_____年_____月_____日

经营期限：_____

姓　　名：_____　　性别：_____　年龄：_____　　职务：____

系_____（供应商单位名称）_____的法定代表人。

特此证明。

法定代表人身份证正面复印件粘贴处	法定代表人身份证反面复印件粘贴处

供应商（公章）：_____

供应商法定代表人签字：_____

日　　期：____年____月____日

法定代表人授权书（适用于授权代表参加投标）

致：明诚汇采项目管理有限公司

我_____系_____的法定代表人，现委派我单位____先生（女士），全权代表我单位处理___项目名称___项目的采购活动（项目编号：_____ ）中的有关事务。本授权书于签字盖章后生效，特此声明。（授权人无转委权）

法定代表人身份证 正面复印件粘贴处	法定代表人授权代表身份证 正面复印件粘贴处
法定代表人身份证 反面复印件粘贴处	法定代表人授权代表身份证 反面复印件粘贴处

附授权代表情况：

姓　名：_____　　性　别：_____职　务：_____

身份证号：_____

通讯地址：_____

邮政编码：_____

电　话：_____（座机）_____

手　机：_____

法定代表人（签字）：_____

法定代表人电话：_____

供应商：____（盖章）____

年　　月　　日

政府采购报价一览表（格式）

供应商名称(盖章)：_____

项目编号：_____

项目名称：_____ **单位：（元）**

序号	内容	投标报价
合计		
投标总价（人民币大写）： 投标总价（人民币小写）：		
项目完成时间：		
优惠条件及备注：		

供应商法定代表人或授权代表签字：_____

职务：_____日期：_____

投标资格证明文件（格式仅供参考）

（1）一般资格要求：供应商符合《中华人民共和国政府采购法》第二十二条规定，并按招标文件要求规范提供下列材料（需加盖供应商公章）。

①具有独立承担民事责任的能力：提供法人或者其他组织的营业执照等证明文件，自然人的身份证明。

②具有良好的商业信誉和健全的财务会计制度：供应商是法人的，应提供 2023 年度(或 2024 年度)经审计的财务报告或基本开户银行出具的 2025 年的资信证明。部分其他组织和自然人，没有经审计的财务报告，可以提供基本开户银行出具的 2025 年的资信证明。

③具有履行合同所必需的设备和专业技术能力：提供具备履行合同所必需的设备和专业技术能力的证明材料或承诺函。

④有依法缴纳税收和社会保障资金的良好记录：提供 2025 年 1 月至今任意三个月缴纳税收的凭据或证明材料复印件(依法免税的供应商须提供相应证明文件)及 2025 年 1 月至今任意三个月社会保障资金缴纳证明材料复印件(不需要缴纳社保资金的供应商须提供相应证明文件)。

⑤参加本次政府采购活动前三年内在经营活动中没有重大违法记录：提供参加本次政府采购活动前三年内在经营活动中没有重大违法记录的书面声明或承诺函。

⑥.法律、行政法规规定的其他条件：供应商需提供承诺函：承诺在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）等渠道查询中未被列入失信被执行人名单、重大税收违法失信主体、政府采购严重违法失信行为记录名单中，如被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单中的供应商取消其投标资格，并承担由此造成的一切法律责任及后果。

⑦本项目不接受联合体

符合相关法律法规及磋商文件规定的其他要求

投标供应商遵守政府采购法规的声明承诺函

致：采购人名称

我单位自愿参加（采购人名称）的（项目名称、项目编号）的投标，并慎重作出如下声明承诺：

一、针对《中华人民共和国政府采购法》

第七十七条 供应商有下列情形之一的，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任：

(一)提供虚假材料谋取中标、成交的；

(二)采取不正当手段诋毁、排挤其他供应商的；

(三)与采购人、其他供应商或者采购代理机构恶意串通的；

(四)向采购人、采购代理机构行贿或者提供其他不正当利益的；

(五)在招标采购过程中与采购人进行协商谈判的；

(六)拒绝有关部门监督检查或者提供虚假情况的。

供应商有前款第(一)至(五)项情形之一的，中标、成交无效。

二、《中华人民共和国政府采购法实施条例》

第十八条 单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

第七十二条 供应商有下列情形之一的，依照政府采购法第七十七条第一款的规定追究法律责任：

(一)向磋商小组、竞争性谈判小组或者询价小组成员行贿或者提供其他不正当利益；

(二)中标或者成交后无正当理由拒不与采购人签订政府采购合同；

(三)未按照采购文件确定的事项签订政府采购合同；

(四)将政府采购合同转包；

(五)提供假冒伪劣产品；

(六)擅自变更、中止或者终止政府采购合同。

供应商有前款第一项规定情形的，中标、成交无效。评审阶段资格发生变化，供应商未依照本条例第二十一条的规定通知采购人和采购代理机构的，处以采购金额 5‰的罚款，列入不良行为记录名单，中标、成交无效。

第七十三条 供应商捏造事实、提供虚假材料或者以非法手段取得证明材料进行投诉的，由财政部门列入不良行为记录名单，禁止其 1 至 3 年内参加政府采购活动。

第七十四条 有下列情形之一的，属于恶意串通，对供应商依照政府采购法第七十七条第一款的规定追究法律责任，对采购人、采购代理机构及其工作人员依照政府采购法第七十二条的规定追究法律责任：

(一)供应商直接或者间接从采购人或者采购代理机构处获得其他供应商的相关情况并修改其投标文件或者响应文件；

(二)供应商按照采购人或者采购代理机构的授意撤换、修改投标文件或者响应文件；

(三)供应商之间协商报价、技术方案等投标文件或者响应文件的实质性内容；

(四)属于同一集团、协会、商会等组织成员的供应商按照该组织要求协同参加政府采购活动；

(五)供应商之间事先约定由某一特定供应商中标、成交；

(六)供应商之间商定部分供应商放弃参加政府采购活动或者放弃中标、成交；

(七)供应商与采购人或者采购代理机构之间、供应商相互之间，为谋求特定供应商中标、成交或者排斥其他供应商的其他串通行为。

三、财政部 87 号令第三十七条 有下列情形之一的，视为投标供应商串通投标，其投标无效：

（一）不同投标供应商的投标文件由同一单位或者个人编制；

（二）不同投标供应商委托同一单位或者个人办理投标事宜；

（三）不同投标供应商的投标文件载明的项目管理成员或者联系人员为同一人；

（四）不同投标供应商的投标文件异常一致或者投标报价呈规律性差异；

（五）不同投标供应商的投标文件相互混装；

（六）不同投标供应商的投标保证金从同一单位或者个人的账户转出。

四、政府采购针对供应商投标行为的其他规定

我公司声明承诺本项目的政府采购投标活动，严格遵守以上政府采购相关法律对供应商投标行为的规定，如声明承诺不实，将承担由此发生的全部法律责任。

投标供应商：（盖章）

日期：　　年　　月　　日

其他材料

服务内容及要求偏离表

项目名称：_____ 项目编号：_____

序号	磋商文件服务要求	投标响应内容	偏离情况	说明
…				
…				
…				
…				

供应商（公章）：_____

供应商法定代表人或其授权委托人签字：_____

日　　期：_____

注：（1）“偏离”系指“正偏离”、“负偏离”或“无偏离”。

（2）请按投标的实际情况，逐条对应招标文件的**“服务内容及要求”**中的要求认真填写该表。

（3）此表可自行扩展。

商务要求偏离表

项目名称：_____ 项目编号：_____

序号	磋商文件商务要求	投标响应内容	偏离情况	说明
…				
…				
…				
…				

供应商（公章）：_____

供应商法定代表人或其授权委托人签字：_____

日　　期：_____

注：（1）“偏离”系指“正偏离”、“负偏离”或“无偏离”。

（2）请按投标的实际情况，逐条对应招标文件的**“商务要求”**中的要求认真填写该表。

（3）此表可自行扩展。

供应商针对评分提供的相关证明材料

一、业绩

二、项目团队

拟投入人员情况表

类别	姓名	职务	职称	专职/兼职	常住地	资格证明（附复印件）			
						证书名称	级别	证号	专业
项目负责人									
技术负责人									
其他人员									

三、其他材料

整体服务方案

（供应商自行制作）

投标声明函

中小企业声明函（货物）

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定，本公司（联合体）参加*（单位名称）*的*（项目名称）*采购活动，提供的货物全部由符合政策要求的中小企业制造。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1.*（标的名称）*，属于*（采购文件中明确的所属行业）行业*；制造商为*（企业名称）*，从业人员人，营业收入为万元，资产总额为万元[1]，属于*（中型企业、小型企业、微型企业）*；

2.*（标的名称）*，属于*（采购文件中明确的所属行业）行业*；制造商为*（企业名称）*，从业人员人，营业收入为万元，资产总额为万元，属于*（中型企业、小型企业、微型企业）*；

……

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

[1]从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

2.残疾人福利性单位声明函

致：_____（采购人名称）_____

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：_____

日　　期：_____

不满足上述条件的供应商可不提供该声明函。

代理服务费确认书（格式）

大成工程咨询有限公司：

若我单位在本次采购活动中成交，在领取成交通知书时将按竞争性磋商文件规定的费率向贵单位支付代理服务费。

供应商：（公章）_____

法定代表人或其授权委托人（签字）：_____

供应商地址：_____

时间：　　年　　月　　日

注：“代理服务费确认书”为响应文件的附件请一同放入响应文件中。

供应商认为有必要说明的其他问题及资料

(格式自拟)

附件（不作为响应文件格式）：

关于印发中小企业划型标准规定的通知

工信部联企业〔2011〕300 号

各省、自治区、直辖市人民政府，国务院各部委、各直属机构及有关单位：

为贯彻落实《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），工业和信息化部、国家统计局、发展改革委、财政部研究制定了《中小企业划型标准规定》。经国务院同意，现印发给你们，请遵照执行。

工业和信息化部

国家统计局

国家发展和改革委员会

财政部

二〇一在合同签定后待收到甲方开工令之日起 90 个日历天安装完成且调试验收合格。六月十八日

中小企业划型标准规定

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》(国发〔2009〕36 号)，制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，**软件和信息技术服务业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。**

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且

营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）软件和信息技术服务业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局 2003 年颁布的《中小企业标准暂行规定》同时废止。