广西壮族自治区政府采购合同

合同名称：广西纪检监察外网改造建设

合同编号：_____

采购单位（甲方）：中国共产党广西壮族自治区纪律检查委员会

住　　所：南宁市锦春路3号

供 应 商（乙方）：中电信数智科技有限公司广西分公司

住　　所：南宁市建信路1号

签订合同地点：广西南宁市

签订合同时间：_____

合同使用说明：根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照招标文件规定条款和中标供应商投标文件及其承诺，甲乙双方签订本合同。

采购合同文本

合同编号：

采购单位（甲方）中国共产党广西壮族自治区纪律检查委员会

采购计划号_____

供 应 商（乙方）中电信数智科技有限公司广西分公司

项目编号 GXZC2025-C3-001506-HCZX

签 订 地 点 南宁市

签订时间 2025 年 月 日

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照招标文件规定条款和中标供应商投标文件及其承诺，甲乙双方签订本合同。

第一条 合同标的

1、服务名称： 广西纪检监察外网改造建设

2、服务数量：详见附件一：响应报价表

3、服务内容：具体详见竞争性磋商文件分标 1 采购需求。

第二条 合同金额

本项目(分标)合同金额(大写)人民币贰佰捌拾万元整

(￥ 2,800,000.00 元)(详见报价表)。

第三条 提交服务成果时间及地点

1、提交服务成果时间：签订合同后 90 个日历日内完成项目建设实施工作，并开展初步验收，2025 年 11 月 30 前申请项目竣工验收。

2、提交服务成果地点：广西南宁市，锦春路 3 号。

乙方所提供的服务必须与招投标文件和承诺相一致且符合相应的服务规范及标准。

第四条　售后服务、质保期

1、乙方应按照国家有关法律法规和“三包”规定以及招标文件、投标文件和本合同所附的《服务承诺》，为甲方提供售后服务。

2、乙方提供的服务承诺、质保期及其它具体约定事项。（见合同附件）

第五条　付款方式

合同生效后 10 个工作日内，采购人向成交供应商支付合同总金额 50%的工程进度款；项目通过初验后，采购人向成交供应商支付支付合同总金额 30%的工程进度款；项目竣工验收，采购人向成交供应商支支付合同总金额 20%作为合同尾款。

第六条　税费本合同执行中相关的一切税费均由乙方负担。

第七条　验收

1. 甲方对乙方提交的服务依据招标文件上的服务要求和国家有关质量标准进行现场初步验收，符合招标文件技术要求的，给予签收，初步验收不合格的不予签收。甲方应当在到中标人的服务成果提交后七个工作日内进行验收。

2. 乙方提交服务成果前应对提交的服务成果作出全面检查和对验收文件进行整理，并列出清单，作为甲方验收和使用的技术条件依据，检验的结果应随服务成果交给甲方。

3. 对技术复杂的服务，甲方应请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。

4. 验收时乙方必须在现场，验收完毕后作出验收结果报告；验

收费用由乙方负责。

第八条　违约责任

1、乙方所提供的服务成果质量不合格的，应及时更换，更换不及时的按逾期提交服务成果处罚；因质量问题甲方不同意接收的或特殊情况甲方同意接收的，乙方应向甲方支付违约服务成果款额 5%违约金并赔偿甲方经济损失。

2、甲方无故延期接收服务成果、乙方逾期提交服务成果的，每天向对方偿付违约服务成果款额3‰违约金，超过 60 天对方有权解除合同，违约方承担因此给对方造成经济损失；甲方逾期付服务成果款的，每天向乙方偿付逾期服务成果款额3‰ 滞纳金。

3、乙方未按本合同和投标文件中规定的服务承诺提供售后服务的，乙方应按本合同合计金额 5‰向甲方支付违约金。

4、乙方提供的服务成果在质量保证期内，因投标人和其它质量原因造成的问题，由乙方负责。

5、其它违约行为按违约服务成果款额5%收取违约金。

6、乙方支付的违约金不足以弥补甲方损失的，还应承担赔偿责任。

第九条 不可抗力事件处理

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。

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。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十条　合同争议解决

1、因服务成果质量问题发生争议的，应邀请国家认可的质量检测机构对服务成果质量进行鉴定。服务成果符合标准的，鉴定费由甲方承担；服务成果不符合标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地人民法院提起诉讼。

3、诉讼期间，本合同继续履行。

第十一条 诉讼

双方在执行合同中所发生的一切争议，应通过协商解决。如果协商不能解决，可向甲方所在地人民法院提起诉讼。

第十二条 合同生效及其它

1．合同经双方法定代表人或授权代表签字或签章并加盖单位公章或合同章后生效。

2．合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3．本合同未尽事宜，遵照《合同法》有关条文执行。

第十三条 合同的变更、终止与转让

1、除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

2、乙方不得擅自转让其应履行的合同义务。

第十四条 签订本合同依据

1、政府采购招标文件；

2、乙方提供的投标文件；

3、成交通知书。

第十五条 双方确认本合同落款通讯地址作为文书送达地址，该通讯地址适用于包括双方合同履行过程中的各类通知、协议等文件以及就合同发生争议进入民事诉讼程序后的一审、二审、再审和执行程序等阶段法律文书的送达。通讯地址需要变更时应当提前 15 个工作日书面通知对方。因提供或者确认的通讯地址不准确、通讯地址变更后未及时依程序告知对方或受送达方拒绝签收等原因，导致文书未能被实际接收的，邮寄送达的，以文书退回之日视为送达之日。

第十六条 本合同一式四份，具有同等法律效力，甲乙双方各两份。本合同甲乙双方签字盖章后生效，自签订之日起七个工作日内，采购人或采购代理机构应当将合同副本报广西壮族自治区财政厅政府采购监督管理处备案。

甲方（章） 年 月 日	乙方（章） 年 月 日
通讯地址：	通讯地址：
法定代表人：	法定代表人：陈善伟
委托代理人：	委托代理人：
电话：	电话：
电子邮箱：	电子邮箱：
开户银行：	开户银行：交通银行北京市分行营业部
账号：	账号：990204011701004601

合 同 附 件

1、供应商承诺具体事项： ①附件一：响应报价表 ②附件二：商务条款偏离表 ③附件三：技术需求偏离表
2、服务具体事项： ①附件四：售后服务承诺书
3、质保期责任：详见附件二：商务偏离表
4、其他具体事项：无

甲方（章）	乙方（章）
年　月　日	年　月　日

注：售后服务事项填不下时可另加附页

附件一：响应报价表

响应报价表

采购项目编号：GXZC2025-C3-001506-HCZX

采购项目名称：广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目

分标号（此处有分标时填写具体分标号，无分标时填写“无”）：分标 1

单位：元

序号	服务名称	数量	单位	单价	总价	备注
1	纪检监察外网商用密码应用安全改造	1	项	2,020,000.00	2,020,000.00	无
2	纪检监察外网安全系统升级	1	项	615,000.00	615,000.00	无
3	机房商用密码应用安全改造	1	项	165,000.00	165,000.00	无
合计金额大写：人民币贰佰捌拾万元整（¥2,800,000.00）						

注：

1. 供应商的报价表必须加盖供应商电子公章，**否则其响应文件按无效响应处理。**

2. 如为联合体竞标，“供应商名称”处必须列明联合体各方名称，标注联合体牵头人名称，**否则其响应文件按无效响应处理。**

3. 如为联合体竞标，盖章处须加盖联合体各方电子公章，**否则其响应文件按无效响应处理。**

4. 如有多分标，分别列明各分标的报价表，**否则其响应文件按无效响应处理。**

供应商名称(电子签章）：中电信数智科技有限公司

日期：2025 年 6 月 20 日

设备清单

序号	名称	设备名称	品牌	规格型号	参数
一	纪检监察外网商用密码应用安全改造	安全认证网关	格尔	SRJ1505-G4020JW	**1.1 安全认证网关**
					提供 2 台安全认证网关，性能需满足但不限于以下内容：
					▲（1）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求，符合 GM/T 0026《安全认证网关产品规范》；（必要项）
					（2）设备应支持与纪检监察部门信息系统进行对接，独立完成纪检监察部门信息系统用户基于证书的身份认证和加密传输；
					（3）支持办公终端防护系统通信交互，实现终端系统全方位防御互动；
					（4）支持纪检监察外网现有应用系统有效结合，为应用系统传递特定的数据信息；本次所有安全认证网关是我司为行业定制版本，结合中纪委身份认证体系可以实现跨省的身份互认，手持一证全国纪委行业可以实现业务认证
					（5）支持纪检监察外网中一次认证，跨应用、跨区域访问的单点登录功能；
					（6）支持标准的协议及数据格式，可方便未来与各种系统及设备进行通信及结合；
					（7）支持多种业务应用：B/S 应用、二层 C/S 应用、三层 C/S 应用等；
					（8）支持多证书链功能；
					（9）支持在线黑名单证书验证，支持海量数字证书黑名单快速检索；
					▲（10）符合国家电子政务外网信任体系并通过国家电子政务外网数字证书中心的 SM2 算法的接入与应用测试；支持与纪委现有电子认证体系互信互认；可支持实现跨省级身份互认互信；
					（11）支持 RSA/SM2 等多种体系自适应；
					（12）支持 SM2、SM3、SM4 等算法，具有密钥协商、身份认证、SSL 隧道加密等功能；
					（13）每秒新建连接数≥5000；最大并发连接数≥1 万。
					▲（14）安全认证网关策略统一下发系统实现客户端策略的统一下发，用户无需对客户端进行任何配置，自治区安全认证网关可以与自治区纪委从 LDAP 和中纪委主 LDAP 同步证书撤销信息，验证证书有效性；可支持实

					现跨省级 LDAP 黑名单列表信息传递；
					▲（15）提供六年质保服务（含软硬件）。
		密码服务管理平台	电科网安	WST-FW-WCSP	**1.2 密码服务管理平台**
					提供 1 台密码服务管理平台，性能需满足但不限于以下内容：
					（1）提供一体机产品形态，支持集群化部署，满足不同场景下的部署需求，2U 机架型，4 个以上 RJ45 10/100/1000M 千兆网络接口；
					（2）支持 SM2、SM3、SM4、SM9 等商密算法；
					（3）支持 RSA、SHA1/SHA224/SHA256/SHA384/SHA512、3DES/AES 等通用算法；
					（4）支持管理的对称密钥数量：5000 万；
					（5）支持每秒并发数 200；
					（6）含密码计算服务、设备与服务管理服务，以及密钥管理服务；
					（7）密码设备与服务管理服务：
					1)租户管理：提供租户新增、编辑、查看、启/禁用、删除等管理功能，以及租户账户管理、授权管理等功能；
					2)密码服务管理：提供密码服务订阅、退订、启用/禁用、查询等管理功能，支持密码服务按需、弹性资源分配，满足动态、差异化需求，支持密码服务的扩容和变更；
					3)应用接入管理：提供应用的新增、编辑、删除、启用/禁用、分组管理、密码服务访问授权等功能，以及通过应用认证和访问控制机制，实现对应用系统调用密码服务的统一管理和控制。（已提供产品功能截图）；
					4)密码设备管理：提供对云服务器密码机、服务器密码机、时间戳服务器等密码设备的接入、使用、管控和状态监控功能，提供密码资源申请、分配、扩容等功能。提供对云服务器密码机池化管理、密码运算资源映射管理、密码资源弹性分配、密码资源智能调度功能。提供对云服务器密码机、虚拟密码机的远程升级能力。（已提供产品功能截图）；
					5)全局监控：可以全局监控平台内所有租户应用信息，如应用名称、所属租户、状态等信息；监控服务信息，如服务在服务器节点上的分布情况、节点资源占用情况、服务状态等信息；监控设备信息，如设备资源占用情况、LB/VSM 虚拟机数量、设备物理和虚拟资源状态等信息。具备告警能力和告警通知能力，提供自定义告警规则可根据提供的数据维度配置告警规则生成告警，提供告警通知规则的配置能力，支持短信、邮件等方式推送告警。支持告警转工单处理能力；

					6)统计报表：提供应用统计、密码服务统计、汇总统计三类报表，支持以租户、应用、密码服务和时间四个维度进度统计。其中应用统计支持应用分布统计、应用交易统计、应用计算接口交易排名、应用密钥使用排名。服务统计模块支持服务交易排名、服务交易结果统计、服务交易趋势、服务交易次数统计、加解密次数统计。汇总统计模块提供租户信息、服务订阅信息、租户加密、解密、签名、验签交易统计信息。（已提供产品功能截图）；
					7)密码监管：提供平台整体服务、应用、密钥和密码计算规格等资源的监测，提供服务交易结果、服务资源异常、应用违规访问等维度的监测能力。提供应用合规自评估和密评风险的能力，可对应用密评合规情况进行自评和应用合规风险进行监测；
					8)管理员管理：提供平台、租户管理员用户个人信息维护、组织机构管理、角色划分、权限划分与授权管理等功能；
					9)日志管理：提供对登录、操作、管理各种管理行为，以及日志备份、恢复各种日志管理的日志记录和审计功能。（已提供产品功能截图）。
					（8）密钥管理服务：
					1)为对称密钥、非对称密钥提供全生命周期管理服务，包括密钥生成、存储、分发、更新、备份、恢复、归档、销毁等功能；
					2)支持算法：支持国密对称密钥（SM1、SM4）、国密非对称密钥（SM2）、国际算法密钥（DES、AES、KDF、RSA、ECC）；
					3)密钥安全：使用三层密钥保护体系安全存储密钥数据，保护密钥存储安全；以应用为单位，对密钥进行细粒度逻辑隔离，保障密钥获取安全；
					4)密钥更新：支持密钥定时更新、按需主动更新，支持密钥更新策略自定义，以及基于多版本机制的统一管理，保障应用的密钥使用安全，特别是当密钥超过使用期限、已泄露、怀疑密钥不安全时（已提供产品功能截图）；
					5)密钥多版本：支持同一密钥唯一标识下密钥的多版本管理。在密钥轮换和更新场景下，无感切换和更新密钥（已提供产品功能截图）；
					6)密钥销毁：支持实时销毁、计划销毁密钥，支持批量销毁密钥。其中计划密钥支持自定义销毁计划，以及销毁计划调整和取消。支持通过接口和管理界面进行密钥销毁管理。（已提供产品功能截图）；
					7)密钥授权：支持同平台跨租户、跨应用的密钥授权，支撑不同应用之间数据互通。密钥的获取需符合授权范

					围要求，防止密钥越权访问和使用。（已提供产品功能截图）；
					8)BYOK 密钥导入：支持两段式密钥导入机制，支持导入其他源产生的密钥；
					9)密钥安全分发：支持基于国密安全传输通道、符合国密相关要求的身份认证、密钥的机密性和完整性保护多重保护机制的密钥安全分发；
					10)密钥备份与恢复：支持定期备份密钥数据，以加密文件形式存储。支持自定义密钥备份策略，支持每天、每周或固定日期备份。备份策略支持启用和禁用两种状态。支持备份密钥文件的下载与恢复；
					11)密钥归档：为到期或销毁的密钥提供安全归档存储服务。支持按密钥销毁时间区间批量归档，支持手动选中指定密钥归档。归档密钥以文件形式存储。支持归档文件的下载；
					12)密钥模版：支持密钥模板的灵活定制，支持自动、手动创建基于模板的密钥服务，简化密钥管理和使用的流程；
					13)证书托管：支持产生 P10 文件。支持托管外部 X509 证书、P12 证书，支持证书的激活、下载、别名修改和详情查看。支持匹配证书内密钥的自动关联；
					（9）含操作系统、数据库、安全容器平台等基础软件；
					▲（10）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书和密码检测报告，适用于 GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（已提供商用密码产品认证证书及检测报告证明材料）；
					▲（11）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书和检验检测报告（已提供检测证书和检验检测报告证明材料）；
					（12）具备全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书，支持 IPV6 协议；
					（13）具备 ITPTC、CMA、CNAS 中国认可检测机构出具的软件测试报告（已提供测试报告证明材料）；
					（14）具备计算机软件著作权登记证书（已提供软件著作权登记证书证明材料）；
					▲（15）提供六年质保服务（含软硬件）。
		签名验签服务器	电科网安	SRJ1912-G	**1.3 签名验签服务器**
					提供 2 台签名验签服务器，性能需满足但不限于以下内容：
					（1）标准 2U 机架型，双电源，4 个 10/100/1000M 自适应电口，可选配 2 个 10G 光口；

					（2）为保护管理账号的安全，多级权限控制：支持管理员、操作员、审计员多级权限控制，保护管理账号的安全；支持管理角色登录口令的有效期控制（已提供产品操作界面截图证明）；
					（3）支持网口绑定，提高设备的服务可靠性（已提供产品操作界面截图证明）；
					▲（4）为确保供应链可靠，硬件采用国产化平台，整机和关键密码部件（密码卡或SE）均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（已提供资质证书证明材料）；
					（5）支持通过管理页面对设备进行在线升级（已提供产品操作界面截图证明）；
					（6）支持金融机构证书414文件批量导入和管理（已提供产品操作界面截图证明）；
					（7）为便于证书管理，支持多机证书自动同步，方便证书管理。可设置设备同步列表，在业务系统通过接口调用导入证书时可将该证书自动同步到其他设备（已提供产品操作界面截图证明）；
					（8）SM2签名/验证:45000/12000次/秒；
					（9）SM3:890Mbps；
					（10）SM4加解密:800Mbps；
					（11）PKCS#1签名/验证：28000/6500次/秒；
					（12）PKCS#7签名/验证：5500/8500次/秒；
					（13）制作信封：890次/秒；
					（14）解析信封：1200次/秒；
					（15）MTBF：≥30000小时；
					▲（16）提供服务：包括设备上架安装，以及对接原数字证书认证系统，接口适配、改造等服务内容；
					▲（17）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，适用于GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（已提供商用密码产品认证证书证明材料）；
					▲（18）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书（已提供检测证书证明材料）；
					（20）具备全球IPv6论坛IPv6 Ready Logo委员会颁发的IPv6 Ready Logo认证证书，支持IPV6协议；
					（21）具备计算机软件著作权登记证书（已提供软件著作权登记证书证明材料）；
					▲（22）能够与广西纪检监察外网部署的原服务器密码设备实现集群部署及对接相关工作，与中央纪检监察外网所部署服务器密码设备实现对接相关工作；
					▲（23）提供六年质保服务（含软硬件）。
		云服务	电	WST-CHSM	**1.4云服务器密码机**

		器密码机	科网安	-XC V1.0	提供2台云服务器密码机，性能需满足但不限于以下内容：
					▲（1）国产化硬件平台；
					（2）2U 机架型，2 个 10G 光口、4 个 10/100/1000M 自适应电口；
					（3）支持 128 个 VSM 自动组成集群，集群内数据自动同步，各 VSM 保持状态一致，提供高可用的密码服务，保障业务的连续性（已提供具备 CNAS 资质检测机构出具的检测报告证明）；
					（4）集群内自动发现功能：零配置，集群内自动发现 VSM，并自动识别 VSM 的权重，简便易用（已提供具备 CNAS 资质检测机构出具的检测报告证明）；
					（5）自动负载均衡功能：集群内置负载均衡，根据自动发现结果，智能负载均衡（已提供具备 CNAS 资质检测机构出具的检测报告证明）；
					（6）弹性伸缩功能：支持单机纵向伸缩，集群横向伸缩，充分利用密码资源，便于业务扩展（已提供具备 CNAS 资质检测机构出具的检测报告证明）；
					（7）可按需创建不同性能/功能/版本的 VSM，满足业务多样性需求（已提供产品功能截图）；
					（8）性能要求（已提供产品功能截图或具备 CNAS 资质检测机构出具的检测报告证明）；
					1)单台设备可创建 VSM 数量 32 个；
					2)SM1 加解密速率 0.6 Gbps；
					3)SM2 签名速率 49,000 次/秒；
					4)SM2 验证速率 38,000 次/秒；
					5)SM3 计算速率 1.5 Gbps；
					6)SM4 加解密速率 1.4 Gbps；
					（9）支持对称算法：SM1/SM4/3DES/AES；支持非对称算法：SM2/RSA2048/RSA4096；支持杂凑算法：SM3/SHA1/SHA256/SHA512；
					（10）支持 VSM 用户独立进行密钥管理；
					（11）提供对使用 VSM 的租户管理员进行智能密码钥匙+证书认证、对业务系统进行证书认证的功能；
					（12）支持不低于 7 种模式的网口绑定，提高设备的服务可靠性，绑定模式可设置（已提供产品操作界面截图证明）；
					（13）提供安全的远程管理功能；
					▲（14）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求（已提供商用密码产品认证证书证明材料）；
					▲（15）采用硬件密码卡，整机和密码卡、管理 USBKEY 均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（已提供硬件密码

					卡、整机、管理 USBKEY 商用密码产品认证证书证明材料）。
					▲（16）提供六年质保服务（含软硬件）。
					▲（17）能够与中纪委服务器密码设备实现对接。
		文件安全存储网关	格尔	KOAL-SBG-S3200	**1.5 文件安全存储网关**
					提供 1 台文件安全存储网关，性能需满足但不限于以下内容：
					▲（1）具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；
					（2）支持国密 SM2/3/4 算法；
					（3）支持基于纪检监察外网商密体系零改造与安全认证设备互动；
					（4）支持为多个应用提供加密服务，且应用拥有独立的文件视图；
					（5）支持多种存储设备，包括 NFS 存储、SAN 存储、GlusterFS 等分布式存储；
					（6）支持为非结构化文件数据（文本文件/办公文件/音视频文件/图形图像文件）、半结构化数据（XML 文件）、结构化文件数据（数据库）提供存储加密服务；
					（7）支持多种部署模式，单节点、双机热备、双活和集群部署；
					（8）支持文件以密文形态进行备份和恢复，支持全量备份和增量备份，支持为不同资源定制备份策略；
					（9）支持兼容多种密码设备，包括加密卡、密码机、云密码机、KMS 密钥管理系统等；
					（10）支持一文一密钥加密；
					（11）使用国密算法对非结构化数据进行加/解密运算，实现数据在存储过程中的机密性保护，SM4 加密 128KB 数据运算平均速率≥1500Mbps，SM4 解密 128KB 数据运算平均速率≥1500Mbps；
					▲（12）提供设备的上架、安装调试，文件服务器的对接适配服务；
					▲（13）提供六年质保服务（含软硬件）。
		数据库加密网关	格尔	KOAL-SBG-D3200	**1.6 数据库加密网关**
					提供 1 台数据库加密网关，性能需满足但不限于以下内容：
					▲（1）具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；
					▲（2）支持纪检监察外网应用系统免改造加密，支持与文件安全存储网关联动实现数据加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数

					据管理；提供灵活的加密状态和非加密状态的双向转换；
					（3）支持对姓名、身份证、手机号码等密文数据进行模糊查询；
					（4）提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次性加密进行加密，加密初始化时使用与字段加密配置一样的加密算法和密钥；
					（5）支持对接入的应用系统进行访问控制，只对授权访问的应用系统提供加解密服务；
					（6）系统可以对数据字段项设置加密规则，提供数据库列级加密，并支持对不同字段列设置不同的密钥和加密算法；
					（7）系统支持 Mysql、Oracle、Sql Server、postgresql、达梦、人大金仓、oceanbase、阿里 rds、华为高斯等多种数据库；
					（8）支持加解密速率≥5600 单元格/秒，支持千万级表；
					▲（9）提供设备的上架、安装调试，数据库服务器的对接适配服务；
					▲（10）提供六年质保服务（含软硬件）。
		目录服务系统	南大	Gbase8d	**1.7 目录服务系统**
					提供 1 套目录服务系统，性能需满足但不限于以下内容：
					▲（1）支持 5000 及以上的条目数据，单个目录服务系统可管理亿级条目；支持精确查询；50 线程，精确查询>10000 次/秒；
					▲（2）提供系统的安装调试以及与广西纪检监察外网部署的原数字证书系统对接适配等服务；
					（3）支持 LDAPV2、V3 标准，包括 RFC2251、RFC2253、RFC2254、RFC2255 及 RFC2256，支持标准的 LDIF 格式；
					（4）提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力；
					（5）支持 PKI 的相关标准，支持 X.509V3 标准，支持 RFC2459、RFC2587 及 RFC3280。
					▲（6）提供三年质保服务（含软硬件）。
		国密浏览器	格尔	SJK-1999	**1.8 国密浏览器**
					提供 20 个国密浏览器授权，性能需满足但不限于以下内容：
					（1）可支持国密应用识别、国密网站标识、国密根证书内置、SSL 双向通信国密加密等功能，实现采用国密算法（SM2、SM3、SM4）应用的网页访问及交互；
					（2）提供软件的安装，终端智能密码钥匙的适配服务；

					▲（3）具备国家密码局商用密码检测中心颁发的浏览器密码模块商用密码产品认证证书；
					（4）支持 HTML 和 CSS 解析，支持 JavaScrip 引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能。
					▲（5）提供三年质保服务。
		智能密码钥匙	龙脉	GM3000	**1.9 智能密码钥匙**
					提供 5000 个智能密码钥匙，性能需满足但不限于以下内容：
					（1）支持 SM2、SM3、SM4 算法，具有身份认证、加/解密、签名/验签等功能；
					（2）提供与原数字证书系统的对接适配，证书在线申请、导入导出等服务；
					（3）用户空间不少于 80K， 数据存储年限不少于 10 年；
					（4）符合 CE 和 FCC 标准；遵循《智能 IC 卡及智能密码钥匙密码应用接口规范》，MS CAPI，X.509 v3 证书存储，SSL v3，IPSec，兼容 ISO 7816；
					▲（5）具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）。
					▲（6）提供六年质保服务。
		密码咨询及网络安全服务	中国电信	定制	**1.10 密码咨询及网络安全服务**
					1.10.1 密码咨询服务
					1.10.1.1 服务内容
					密码政策与标准咨询：国家对密码管理出台了多项法律法规，如《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等。通过该服务，对这些法律法规进行深入解析，帮助准确理解密码政策的核心要求，从而确保其在系统设计、运营和维护中保持合规。
					应用系统开发改造对接：根据现有系统架构，设计密码应用的对接方案，确保新密码系统与原有系统的兼容性。
					密码系统评估与优化：对现有的密码系统进行全面的安全预评估，确保系统在安全性、可用性、合规性等方面满足要求。
					密码技术培训与指导：为技术团队提供密码技术的基础培训，确保被培训人员能够理解和掌握密码系统的核心概念和技术操作。
					1.10.1.2 服务范围
					密码咨询服务将帮助自治区纪委监委优化现有密码技术体系、密码管理体系，确保单位内的相关应用系统密码应用的合规性、有效性、正确性。
					1.10.1.3 服务频率

					项目期内提供 1 次。
					1.10.1.4 服务交付物
					《政策解读与标准对接报告》、《密码应用方案设计文档》、《应用系统改造对接文档》、《码系统评估与优化报告》、《密码技术培训资料》等。
					1.10.2 安全漏洞扫描服务
					1.10.2.1 服务内容
					主要是通过安全评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，查找 WEB 应用系统、服务器主机、数据库等安全对象目标存在的安全风险、漏洞和威胁。
					1.10.2.2 服务范围
					对单位已授权的网络安全设备、操作系统、数据库、中间件和 WEB 应用系统进行漏洞扫描。
					1.10.2.3 服务频率
					项目周期内提供 2 次漏洞扫描服务。
					1.10.2.4 服务交付物
					《漏洞扫描工作方案》、《漏洞扫描授权书》、《安全测试授权函》、《漏洞扫描报告》、《漏洞风险跟踪台账》等。
					1.10.3 风险评估服务
					1.10.3.1 服务内容
					通过风险评估服务，全面、准确的了解被评估信息系统的安全现状、发现系统可能会出现的安全问题，保证系统处于一个高度可信任的状态。在等级保护测评工作的基础上，针对测评对象实施网络安全风险评估服务，以测评发现的技术与管理结果作为风险评估服务输入，结合风险评估标准化流程开展网络安全风险评估服务工作。主要包括如下内容：
					1.10.3.1.1 资产识别及赋值
					进行资产识别及赋值，确定组织和信息系统中的资产，明确资产价值以及相应的保密性、完整性、可用性等安全属性情况，连接资产之间的相互关系和影响，识别出重要资产，进行赋值与计算生成《资产价值分析报告》。
					1.10.3.1.2 威胁识别及赋值
					进行威胁识别及赋值，明确存在的威胁及其发生的可能性，以及严重威胁说明，生成《威胁分析报告》。脆弱性识别及赋值
					进行脆弱性识别及赋值，脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性涉及安全组织、安全策略、安全制度、人员安全、系统运维等方面的安全问题。根据脆弱性被威胁利用所产生的后果对脆弱性进行赋值分析，生成《安全技术脆弱性分析报

					告》和《安全管理脆弱性分析报告》。
					1.10.3.1.3 现有安全控制措施分析
					分析组织或信息系统已部署安全措施的有效性，包括技术和管理两方面的安全管控分析，生成《已有安全措施分析报告》。
					1.10.3.1.4 风险分析
					在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，对资产、威胁、脆弱性等评估数据进行关联计算、分析评价，生成《风险评估报告》。
					1.10.3.2 服务范围
					通过前期调研问询确定风险评估范围为：应用系统所涉及的服务器（应用以及数据库）、中间件、数据库、数据资产以及相关管理人员、网络防护设备以及安全管理制度。
					1.10.3.3 服务频率
					项目期内提供一次。
					1.10.3.4 服务交付物
					《资产价值分析报告》、《安全技术脆弱性分析报告》、《安全管理脆弱性分析报告》、《已有安全措施分析报告》、《风险评估报告》等。
					1.10.4 渗透测试服务
					1.10.4.1 服务内容
					渗透测试服务是模拟黑客的思维和攻击手法，采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试，以真实有效的发现应用系统可能存在的安全漏洞，有效帮助用户识别应用系统安全风险，提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展，主要的测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等，并指导、协助开发运维单位修复漏洞。
					1.10.4.2 服务范围
					服务范围≥6 个业务系统。
					1.10.4.3 服务频率
					项目期内提供一次。
					1.10.4.4 服务交付物
					《渗透测试报告》等。
					1.10.5 应急响应服务
					1.10.5.1 服务内容

					针对突发事件，提供网络攻击行为、网络攻击事件应急响应处置和溯源分析服务，协助分析攻击来源、分析事件原因，编制事件应急处置防守报告；根据单位环境和需求，按照桌面推演或模拟演练的方式，选定 1 个特定网络安全威胁场景，协助编制网络安全应急预案，搭建模拟场景的演练环境，协同用户编制演练脚本，并按照演练方案和演练脚本组织开展应急演练工作，演练完成后，协助用户编制应急演练报告，对存在的问题指导完善应急机制和流程。
					1.10.5.2 服务范围
					提供 1 个场景的应急响应服务。
					1.10.5.3 服务频率
					项目期内提供 1 次服务。
					1.10.5.4 服务交付物
					《应急响应（处置）报告》、《应急预案》、《应急演练方案》《应急演练报告》等。
					1.10.6 安全意识培训服务
					1.10.6.1 服务内容
					面向单位普通职工开展 1 次集中化的信息安全意识培训，培训内容根据单位的需求可包括网络安全法律法规解读、典型网络安全事件分析、常见网络安全风险介绍以及个人信息安全防护技巧等内容，通过培训宣讲增强全体人员的网络安全意识和防范技巧，提供单位整体安全防护能力。
					1.10.6.2 服务范围
					主要面向反腐倡廉网络信息中心、党风廉政教育中心的网络和系统相关管理人员，委机关其它人员自愿原则参加。
					1.10.6.3 服务频率
					项目期内提供 1 次。
					1.10.6.4 服务交付物
					《安全培训方案》、《安全培训 PPT》、《培训签到表》等。
					1.10.7 数据安全管理体系建设服务
					1.10.7.1 服务内容
					通过识别、评估、控制和监测数据生命周期中的各个环节，确保数据的机密性、完整性和可用性。该服务包括策略制定、流程优化、技术部署、数据分级分类、人员培训及应急响应机制建立等关键要素，构建符合行业标准和法规要求的数据安全管理体系，有效防范内外部威胁，保障业务连续性。
					1.10.7.2 服务范围
					涵盖了组织建设、制度流程、技术工具以及人员能力等多个方面。

					1.10.7.3 服务频率
					项目期内提供 1 次服务。
					1.10.7.4 服务交付物
					《数据安全管理方案》等。
		数据库管理系统 A	达梦	达梦数据库管理系统[简称：DM]V8.4	**1.11 数据库管理系统 A**
					提供 4 套数据库管理系统，性能需满足但不限于以下内容：
					（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。
					（2）支持多种云计算基础设施环境，支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。
					（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；
					（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。
					（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存储引擎表的混合查询。
					（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。
					（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；
					（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。
					（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移；已提供专业测评

					机构出具的测试报告。
					（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大规模并行处理集群、读写分离集群、主备集群。
					（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。
					（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。
					（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。
					（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。
					（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。
					（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。
					（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；
					▲（18）落盘数据的“全面加密”。无论是数据文件，还是日志文件、备份文件、导入导出文件，均支持透明的存储加密。在国产 CPU 环境下的第三方专用密码设备支持；
					▲（19）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，已提供专业测评机构出具的测试报告。

					（20）数据库具备高安全性，已提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印件。
					▲（21）应与中央纪委统建业务应用系统适配。
					▲（22）提供原厂三年质保服务。
		数据库管理系统 B	电科金仓	金仓数据库管理系统 Kingbase ES V8.0	**1.12 数据库管理系统 B**
					提供 1 套数据库管理系统，且与数据库管理系统 A 异构，性能需满足但不限于以下内容：
					（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。
					（2）支持多种云计算基础设施环境，支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。
					（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；
					（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。
					（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存储引擎表的混合查询。
					（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。
					（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；
					（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。
					（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、

					重命名等分区操作；支持分区表迁移；已提供专业测评机构出具的测试报告。
					（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大规模并行处理集群、读写分离集群、主备集群。
					（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。
					（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。
					（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。
					（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。
					（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。
					（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。
					（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；
					▲（18）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，已提供专业测评机构出具的测试报告。
					（19）数据库具备高安全性，已提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印件。
					▲（20）应与中央纪委统建业务应用系统适配。

					▲（21）提供原厂三年质保服务。
		数据守护集群软件	达梦	达梦数据守护集群软件[简称：DMDataWatch]V8.10	**1.13 数据守护集群软件**
					提供 4 套数据守护集群软件，性能需满足但不限于以下内容：
					为确保系统运行稳定，所提供集群软件和数据库管理系统 A 同一品牌；
					▲（1）提供全功能的数据库双机热备能力，完全支持单机一致的功能，不依赖于第三方集群组件，支持备机可读。可在不停机状态下在单机系统与主备系统间平滑变换，备机时刻保持与主机的数据同步。一旦主机发生故障，备机立刻可以自动切换成新的主机，继续提供服务，同时支持客户端透明切换。
					（2）支持一主多备，支持同步备机和异步备机等多种方式，支持备机只读，支持备机中创建使用临时表，支持列存表。
					（3）数据库集群提供负载均衡能力和故障隔离能力，可根据场景调整负载均衡策略。
					（4）数据库集群提供高可用性，支持秒级的故障快速切换。
					▲（5）数据库集群具有可扩展性，可随着用户访问量增加，对集群进行扩容，增加节点以提高。
					▲（6）提供原厂三年质保服务。
		中间件	金蝶	金蝶 Apusic 应用服务器软件 V10	**1.14 中间件**
					提供 3 套中间件，性能需满足但不限于以下内容：
					（1）支持主流硬件，如 Intel、AMD、龙芯、飞腾、鲲鹏、兆芯、海光、申威等；
					（2）支持主流操作系统，如 Redhat、CentOS、Windows、中标麒麟、统信 UOS、银河麒麟、深度、普华等；
					（3）支持主流数据库，如 OracleDB、MySQL、GaussDB、OceanBase、达梦、金仓、神通、南大通用、瀚高等；
					（4）产品具有等保密级功能，可通过 B/S 管理控制台对应用的密级标识进行选择，密级标识应与信息主体不可分离，密级标识应不得篡改
					（5）中间件产品技术成熟稳定，具有国际领先性与影响力，中间件产品连续四年入选 Gartner 企业级应用服务器魔力象限，已提供官网截图证明材料。
					▲（6）产品具有访问控制功能，实现等保三员功能，系统管理、安全管理和安全审计三权分立；
					（7）为实现对部分老版本应用系统的兼容支持，产品需支持 JavaServer Faces（JSF）标准功能框架，且同时支持在 JSF 中，可执行动态方法，中间件产品需要提供相关的支持方法及组件模块，已提供证明材料；
					▲（8）提供原厂三年质保服务。
二	纪	升级远	绿	绿盟	**2.1 升级远程安全评估系统**

	检监察外网安全系统升级	程安全评估系统	盟	RSASNX3-S	提供1套远程安全评估系统的升级服务，服务需满足但不限于以下内容：
					（1）可全方位系统脆弱性发现，全面发现信息系统存在的安全漏洞、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。
					（2）能从海量数据中快速定位风险，提供仪表盘报告和分析方式，在大规模安全检查后，快速定位风险类型、区域、严重程度，根据资产重要性进行排序，可以从仪表盘报告直接定位到具体主机具体漏洞。
					（3）支持检测的漏洞数大于300000条，兼容CVE、CNCVE、CNNVD、CNVD等主流标准。
					（4）内置不同的漏洞模板针对Unix、Windows操作系统、网络设备和防火墙等模板，同时支持自定义扫描范围和扫描策略；
					（5）能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程中的漏报和误报。
					（6）支持手动和自动升级。自动定时升级支持Http代理方式，立即升级支持一键式更新。
					（7）升级完成后的设备包含四年系统漏洞软件特征升级服务，以及四年软件升级和硬件质保服务。
		升级安全感知系统平台	深信服	深信服安全感知系统平台特征库软件V2.0	**2.2升级安全感知系统平台**
					提供1套安全感知系统平台的升级服务，服务需满足但不限于以下内容：
					（1）开启主机类资产识别模块，能够识别资产数据来源、IP地址、主机名、MAC地址、基线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP类型、识别方式、首次发现时间等；
					（2）开启挖矿专项检测模块，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息；
					（3）开启自定义分支管理模块，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等；

					（4）开启威胁定性模块，支持以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；
					（5）开启责任人管理模块，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自动识别资产图库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理；
					（6）开启安全态势的大屏模块，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；
					（7）开启弱密码扫描模块，支持 SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL 等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web 空密码等；
					（8）开启报表分析模块，可快速生成月度、季度、年度 PPT 报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，可直接通过导出的 PPT 报告进行工作汇报，帮助用户进行高效工作，体现安全工作价值；
					（9）开启联动响应模块，要求支持与同品牌防火墙、行为管理、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等；
					（10）支持 ATT&CK 检测模块，基于 ATT&CK 能力图谱将网络安全现状映射到模型的各个阶段，支持命中攻击技术统计展示，支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产；

					（11）支持潜伏威胁黄金眼模块，支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入 IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点；
					（12）支持 EBA 实体行为分析模块，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常横向访问等；
					▲（13）提供三年硬件维保、软件升级、规则库更新服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。
		升级感知系统探针	深信服	深信服安全感知系统探针特征库软件 V2.0	**2.3 升级感知系统探针**
					提供 1 套安全感知系统探针的升级服务，服务需满足但不限于以下内容：
					（1）开启报文检测引擎模块，可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。
					（2）开启 WEB 智能检测模块，支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。
					（3）开启网站攻击防御模块，支持 XSS 攻击、网页木马、网站扫描、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。
					（4）开启敏感信息检测模块，对敏感信息进行检测，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计 2 种方式进行命中次数统计。

					（5）开启漏洞利用攻击检测模块，支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。
					（6）开启智能语义引擎检测模块，可针对 http 隧道、java 反序列化保护等类型进行自定义设置。
					（7）开启网络拓扑扫描模块，支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况；
					（8）开启弱口令检测模块，支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型(FTP/WEB 登录）的爆破次数；
					（9）开启僵尸网络检测模块，支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。
					（10）开启多种类型日志传输模式授权，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
					（11）开启暴力破解检测模块，支持 FTP、IMAP、MS Sql、Mysql 、Oracle 、Discuz 、Basic Authorization 、Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat、Sybase、Weblogic 、Wordpress 、VNC 等 73 种协议暴力破解检测；
					（12）开启传输协议审计模块，支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。
					（13）支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
					（14）新增自定义应用识别规则库模块，可以通过参数的灵活设定，把关注的特殊事件作为自定义策略下发给引擎进行检测。对于网络流量的异常情况具有非常准确、有效的发现能力。
					▲（15）提供三年硬件维保、软件升级、规则库更新等服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。

		升级日志审计系统	安恒	DAS-LOG-460	**2.4 升级日志审计系统**
					提供 1 套日志审计系统的升级服务，服务需满足但不限于以下内容：
					（1）系统在功能性升级增加了大数据底层架构，全面日志各类安全日志接入，包括第三方网络设备、安全设备、主机日志信息等；
					（2）升级后系统支持多维度安全风险展示，可通过系统强大的数据分析能力，进行多资产数据、安全告警数据聚合，发现潜在的安全问题，利用内置的多种分析规则，对数据进行多维度关联分析；
					（3）系统升级后支持高效的全文检索引擎，支持从亿级日志信息中秒级响应检索结果，支持基于关键字、多种逻辑关系符的组合运用精确查询。
					（4）提供维保设备故障应急处置预案，并按预案及时解决设备故障，保障设备的高可用性，确保设备稳定运行。
					（5）定期远程巡检和维护，根据要求对设备进行远程巡检和预防性维护，并对巡检中发现的问题给与及时修复，每年度至少提交两次书面巡检报告。
					（6）移机技术支持服务，提供设备系统移机技术支持服务，且对设备进行安装调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的调试等。
					▲（7）对日志审计系统软件进行维保升级，升级内容包括三年硬件质保服务及软件、特征库升级更新服务。
		升级防火墙系统	奇安信	NSG5000-TG20	**2.5 升级防火墙系统**
					提供 2 套防火墙系统的升级服务，服务需满足但不限于以下内容：
					1、升级后的系统集成防火墙、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，可实现对威胁的分析、定位、处置一体化过程。具体功能如下：
					（1）基础防火墙功能：支持多种形式灵活部署，具备访问控制、负载均衡、VPN、虚拟系统、高可用性等功能，并可防护扫描、泛洪、异常数据包等传统网络攻击。
					（2）防病毒：支持对 HTTP、FTP、POP3、SMTP、IMAP、SMB、IPTUX 七种协议进行病毒查杀。
					（3）入侵防御：支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL 注入、WEB 攻击、弱口令扫描等入侵行为防御。
					（4）虚拟系统：支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。

					（5）行为管理：支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。
					（6）应用层内容安全防护：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。
					（7）威胁情报：支持本地+云端威胁情报联动能力，本地威胁情报支持手动和自动升级。
					（8）应用识别与控制：支持精确识别 5000 余种应用，支持应用云识别。
					（9）URL 过滤：支持手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。
					▲2、升级完成后的设备包含三年威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级、授权服务，以及三年软件升级和硬件质保服务。
		升级安全准入网关	天融信	SJJ1995-42706	**2.6 升级安全准入网关**
					提供 2 套安全准入网关的升级服务，服务需满足但不限于以下内容：
					（1）SSL VPN 升级模块，使原有 VPN 设备支持 SSL VPN 功能；
					（2）开通授权升级模块，提供 205 个 SSL VPN 客户端许可；
					（3）支持主从认证账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定；
					（4）符合国密局制定的《SSL VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4；
					（5）支持 WEB 转发、端口转发、全网接入模式；端口转发模式支持 TCP、UDP 协议；
					（6）支持智能递推；
					（7）客户端支持主流 Windows 系统、MAC 系统、Linux 系统（含 Cent OS、Ubuntu、银河麒麟、优麒麟等）；
					（8）兼容多种类型浏览器，包括 IE6、7、8、9、10、11，Chrome、Opera 、Safari、Firefox；
					（9）支持多线路源路返回的智能选路；
					（10）支持双机热备模式下的授权漂移，仅需采购一套接入许可；
					（11）支持 SSL VPN 会话状态监测；
					（12）支持通过 WebCache 技术对 web 页面进行数据优化，支持智能压缩技术，减少不必要的数据传输；
					（13）支持 HTTP401 方式、WEB 方式、密码助手方式的单点登录，用户登录 VPN 后无需二次认证，即可登录内

					部 B/S、C/S 应用系统，支持用户修改单点登录的账户信息；
					（14）支持基于 Android/ IOS 平台的第三方软件开发包（SDK），用于封装第三方应用软件（APP），无需安装独立客户端，即可实现数据加密传输，业务安全接入；
					（15）支持针对 Android 平台 APP 的 VPN SDK 自动打包；
					（16）支持 iOS、Android 智能终端以及 Windows 系统的虚拟桌面与虚拟应用发布方式接入，实现数据不落地，有效保证数据安全；
					（17）支持 iOS、Android 智能终端的全网接入模式（非 PPTP 方式）；
					（18）支持用户名/口令、CA 证书、指纹识别、人脸识别、USB KEY、短信认证、动态令牌、硬件特征码、图形码认证；
					▲（19）提供三年软件升级和硬件质保服务。
		升级出口 vpn	深信服	升级服务	**2.7 升级出口 vpn**
					提供 1 套出口 vpn 的升级服务，服务需满足但不限于以下内容：
					（1）开启单点登录功能模块，支持移动用户登录 VPN 后再登录内部 B/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全。
					（2）开启断线重连模块，防止用户误操作关闭浏览器导致 VPN 隧道断开；防止用户在无线网络环境下网络正常切换时 VPN 隧道断开；
					（3）支持环境检测、自动修复模块，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。
					（4）开启用户/用户组细粒度的权限分配模块：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。
					（5）开启基于硬件指纹特征的认证模块，可实现用户与终端的绑定，支持终端接入审批，仅允许审批通过的终端接入 VPN；支持用户自助审批；支持设置用户可允许接入的终端数量；
					（6）开启基于 PKI 体系的第三方 CA 进行结合认证模块 ，可根据 CA 某字段将通过 CA 认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表。
					（7）开启系统实时监控模块，图形化显示一段时间内的运行状况，可查看 CPU 占用率、各条线路网络吞吐量、各条线路的 IP 地址及发送接收流速、并发会话数、SSL 并发用户数；可查看历史最高并发用户数并显示时间记

					录；可实时查看 SSL 接入用户的用户名、接入时间、接入 IP、虚拟 IP、认证方式等信息，并可在线中断指定用户；
					（8）开启独立日志中心模块，进行 SSLVPN 实时日志记录，可详细记录用户访问资源记录（用户、主机 IP、资源、时间）、管理员日志（管理员、主机 IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机 IP 等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆 SSLVPN 采用非绑定账号访问应用系统的记录 ；
					（9）开启备份模块，支持 SSLVPN 配置的单独备份、恢复功能，并支持历史配置的回滚 ；
					▲（10）提供三年硬件维保、软件升级、规则库更新，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。
		新增流量采集探针	绿盟	UTSNX3-HD4100-P	**2.8 新增流量采集探针**
					提供 1 套流量采集探针，性能需满足但不限于以下内容：
					（1）为软硬一体化 2U 标准机架式设备，标配 4 个千兆电口和 2 个扩展槽位，双电源，硬盘 24T，内存 32G，内置沙箱 1 个；
					（2）吞吐量：1.5Gbps；
					（3）支持多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等，能够自动解析 DNS 响应的矿池及 IP 地址；
					（4）支持 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP 等多种协议报文识别，支持≥1000 种应用识别；
					（5）具有文件威胁检测能力，能够准确识别≥300 种文件类型；支持恶意程序分类；针对检测出的恶意文件，能够给区分类型，如木马、勒索病毒等等；能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等；
					（6）支持对 Web 攻击、漏洞利用、恶意软件、隐蔽隧道、黑客工具、内网安全等多种类型威胁检测；

					（7）提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持 WinXP、Win2003 & 2008 & 2012 server、Win7 & Win10 等主流 Windows 平台沙箱镜像；能够集成外接沙箱分析系统，提高未知威胁分析处理能力（已提供功能界面截图证明）；
					（8）内置沙箱能够对未知漏洞利用代码和恶意程序的进程操作行为、文件操作行为、系统配置操作行为、网络通信行为、恶意未知威胁逃逸行为等进行动态分析（已提供功能界面截图证明）；
					（9）支持未知威胁事件证据留存，提供样本分析报告，报告内容包括：样本基本信息、执行后行为记录、重点标注恶意行为；
					（10）支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，提高运维效率；
					（11）支持 RSA、国密 SM2 加密算法的服务器私钥导入进行加密报文的解密后检测；
					（12）具备 DNS 协议解析功能，发现发起 DGA 域名请求的失陷主机；
					（13）具备威胁情报 IOC 检测能力，威胁检测类型包括：远控、钓鱼、僵尸网络、矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、黑客工具、APT 攻击事件、流氓推广、其他恶意软件等；支持域名、URL、IP 类型的威胁情报检测，对 IP 情报可以精确到端口级别；支持和威胁情报云端联动，有效检测新威胁；
					（14）能够对相同攻击源、攻击目标、攻击类型的事件告警进行聚合，减少不必要的重复告警；内置自动研判功能，能够对攻击方向、攻击结果进行自动判定，并在告警中展示攻击结果；
					（15）支持以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载；
					（16）支持通过解析流量中的 IP 地址、端口号和应用层协议，自动识别网络资产，包括服务器类、网络设备类、终端类资产，并能够对资产进行分组管理，编辑资产信息，包括资产名称、是否核心资产等；
					（17）支持自动发现存在弱密码账号的资产，展示相关资产信息、以及存在弱密码的账号、密码、协议和登录端口，能够对密码进行脱敏存储和展示；
					（18）支持大屏展示，可视化展示威胁分类统计数据、排名前五的病毒事件、失陷风险最高的 TOP5 主机、攻击源和攻击目标地理位置等内容；
					（19）支持预设报表，包括日报、周报、月报，并支持自定义报表生成时间；

					（20）支持日志管理，可依据受害者 IP、攻击者 IP、文件名称、MD5 等查询条件查询日志；支持 Syslog 协议，可以实时传输日志到 syslog 服务器，选择传输的内容类型；支持同时上传多个日志服务器；
					（21）为保证系统稳定性和兼容性，探针必须能够与纪检监察外网现有态势感知平台对接，满足流量采集、关联分析和溯源取证要求；
					▲（22）提供六年产品及授权维保服务。
		新增万兆防火墙	绿盟	NFNX5-HDX2000	**2.9 新增万兆防火墙**
					提供 2 套万兆防火墙，性能需满足但不限于以下内容：
					（1）应用层吞吐量 18Gbps，规格：2U，内存大小 16G，硬盘容量 256G SSD+4T 机械硬盘，电源：冗余电源，接口 6 个千兆电口，4 个千兆光口 SFP，4 个万兆光口 SFP+(含 4 个万兆光模块)，并发连接数 800 万，HTTP 新建连接数 25 万，IPSec VPN 最大接入数 1500；
					（2）具备防病毒功能模块及授权，且吞吐量性能 10G；
					（3）具备 IPS 功能模块及授权，且吞吐量性能 12G；
					（4）具备网关杀毒功能模块及授权，且吞吐量性能 6G；
					（5）具备全威胁处理能力模块及授权（含应用防护功能），且吞吐量性能 6G；
					（6）具备 IPSec VPN 能力模块及授权，且吞吐量性能 4G（AES256）或 1G（国密 SM3/SM4）；
					（7）能够对设备环境、基础产品信息、安全性、稳定性、硬件健康状态、平台及软件健康状态进行监测，并每季度提供巡检服务并出具巡检报告；
					（8）提供 7*24 小时 400 热线（400-818-6868）优先接入权益；
					（9）提供用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；
					（10）提供策略生命周期管理功能，对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；
					（11）提供内置漏洞规则，同时要在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，用户可以自定义 IPS 规则；
					（12）支持对具有攻击行为的 IP 采取临时禁封和永久禁封两种处理模式，IP 临时禁封功能能与设备安全防护规则实现联动；（已提供产品操作界面截图证明）
					（13）支持封堵 IP 记录数量≥5 万；

					（14）针对 http 应用攻击行为日志，支持可查看攻击请求原始报文内容，包括请求头信息及 payload 详细信息等，便于专业技术人员进行分析和研判；（已提供产品操作界面截图证明）
					▲（12）提供六年硬件设备故障返厂维修服务、三年软件升级服务、三年规则库更新、三年病毒库更新、三年 URL 更新。
三	机房商用密码应用安全改造	安全加固网关	中星电子	VS-GW8004S(V2F1V5)	**3.1 安全加固网关**
					提供 4 套安全加固网关，性能需满足但不限于以下内容：
					（1）摄像机接入能力支持≥1 路通用网络摄像机接入；
					（2）支持摄像机接入协议包括 GB/T 28181、ONVIF、RTSP 等；
					（3）支持接入视频分辨率最高 4096x2160@30fps；
					（4）接入视频编码格式 H.264/H.265；
					（5）输出视频编码格式支持 GB/T 25724-2017(SVAC2)；
					（6）输出视频分辨率包括 1920x1080P@30fps、2560x1440@30fps 等可供选择；
					（7）信息安全：支持 GB 35114（达到最高安全等级 C 级要求），支持视频数据签名认证和加密（已提供公安部出具的检测报告证明材料复印件）；
					（8）网络接口：2 个，RJ45 10M/100M 自适应以太网口，支持物理隔离（如：1 路下联网络摄像机，1 路上联 GB 35114 平台）；
					（9）供电：DC12V-2A；
					（10）最大功耗：12W；
					（11）工作温度范围：-40℃～＋70℃；
					（12）工作湿度范围： 0%～90%，无冷凝；
					（13）提供设备的安装调试以及与原机房摄相机的线路改造服务。
					（14）提供三年质保服务。
		智能密码钥匙	天津赢达信	VS-UKEY-01	**3.2 智能密码钥匙**
					提供 1 个智能密码钥匙，性能需满足但不限于以下内容：
					（1）支持与 CA 系统协同颁发数字证书；
					（2）非对称运算（SM2）：5 次/秒；
					（3）支持对称运算（SM4）：20Mbps/秒；
					（4）可支持的操作系统：win7 32/64 位、Linux 等；
					（5）提供与原数字证书系统的对接适配，证书导入导出等服务。
					（6）提供三年质保服务。
		安全智能视频	中星	SIVS708-B(Z1T4)	**3.3 安全智能视频一体化服务系统**
					提供 1 套安全智能视频一体化服务系统，性能需满足但

		一体化服务系统	电子		不限于以下内容：
					1、功能要求：
					（1）视频编解码支持 SVAC2.0 国家标准，兼容支持 H.264、H.265 标准（已提供检测报告证明材料）
					（2）信息安全标准支持 GB35114-2017，支持视频认证和加密，达到最高安全等级 C 级要求；（已提供公安部出具的检测报告证明材料复印件）
					（3）支持 IPC 设备通过 GB/T28181 协议、ONVIF 协议联网接入
					（4）支持 8 路 GB35114 A\B\C 级前端接入
					（5）WEB 客户端实时视频浏览，支持 1、4、6、9、13、16、25 多种分屏模式下实时视频浏览
					（6）支持 WEB 客户端录像回放，多种倍速回放，支持 WEB 客户端事件查询，报警信息查询
					（7）商密认证要求：内置 UKEY 符合安全二级及以上，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性，满足密码测评要求符合商用密码产品认证证书、并符合 GM/T0028《密码模块安全技术要求》安全等级二级及以上的相关要求、支持 GB/T 39786-2021 第三级及以上密码应用基本要求的规定。（已提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。
					2、硬件参数要求：
					（1）机型：2U
					（2）盘位：8 盘位；
					（3）接入 32Mbps，储存 32Mbps，转发 16Mbps；
					（4）支持 4 路录像回放（单路 4Mbps 1080P）；
					（5）WEB 单客户端支持 4 路 1080P 4M 码流解码；
					（6）WEB 客户端支持 35114 验签及解密播放；
					（7）使用国密标准的 UKEY；
					（8）显示输出接口：1 个 VGA，2 个 HDMI；
					（9）网口:2 个千兆网口；
					（10）提供设备的安装调试等服务。
					（11）提供三年质保服务。
		安全智能人脸门禁	重庆中星微	VM-ACT070-YD(V3)	**3.4 安全智能人脸门禁**
					提供 1 套安全智能人脸门禁，性能需满足但不限于以下内容：
					（1）国密安全门禁系统完全符合 GM/T0036《采用非接触卡的门禁系统密码应用技术指南》，采用国产密码算法对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，同时对门禁记录的完整性进行保护，可应用于等保三级（及以上）信息系统的等保、密评建设和整改需求。（已提供国家密码管理局商用密

					码检测中心颁发的门禁系统类商用密码产品认证证书复印件）
					（2）采用国产芯片，国密算法，保障门禁系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性要求；信息安全标准支持 GB35114-2017 C 级安全要求；（已提供公安部出具的检测报告证明材料复印件）
					（3）具有抓拍功能，除了抓拍正常刷脸或者刷卡开门照片上传到后台以外，还具有陌生人抓拍预警功能；
					（4）支持人脸识别加刷卡双因子认证开门方式，保证人证合一，有效防止门禁卡被乱用或者盗用；
					（5）内置双目近红外摄像头，基于光流分析的人脸识别技术，防止照片、视频攻击；
					（6）门禁基本参数：内存 1G，存储 1G +16G 扩展储存，验证开门方式支持刷卡、人脸识别、刷卡+人脸识别；人脸比对速度：白天＜500ms 夜间＜900ms，人脸特征值存储容量 3000 条，CPU 卡存储容量 3000 条，显示屏：7 寸，分辨率：1024*600，工作电压：12V±10%，工作电流 1.5A，门锁控制方式：RS485，使用环境范围：-10~+60℃，安装方式：壁挂。
					（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。
					（8）提供三年质保服务。
		门禁控制器	重庆中星微	VM-AC2-YD11	**3.5 门禁控制器**
					提供 1 个门禁控制器，性能需满足但不限于以下内容：
					（1）制门锁的执行单元，内置国家密码局认证的安全芯片，采用国密算法与门禁机前端进行加密通讯；
					（2）功能：单/双门单门禁机（单向），单/双门双门禁机（双向），1 路门状态反馈，1 路报警输入，RS485 通讯方式；
					（3）门禁控制器包括：门禁控制模块、门禁电源、漏电开关、接地排，门禁控制器机箱；
					（4）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。
					（5）提供三年质保服务。
		双门磁力锁	国产	定制	**3.6 双门磁力锁**
					提供 1 个双门磁力锁，性能需满足但不限于以下内容：
					（1）双门磁力锁，DC12V，LED 指示灯，门状态反馈，适合木门，铁门，有框玻璃门等。适合标准安装，门关上后门框上有固定磁力锁的位置；
					（2）提供原门禁系统的拆除或利旧，以及新门禁系统

					的综合布线等安装调试服务。
					（3）提供三年质保服务。
		开门按钮	国产	定制	**3.7 开门按钮**
					提供 1 个开门按钮，性能需满足但不限于以下内容：
					（1）出门开关，ABS 阻燃塑料，白色，螺丝固定穿墙安装或配备明装 86 底盒；
					（2）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。
					（3）提供三年质保服务。
		玻璃破碎紧急按钮	国产	定制	**3.8 玻璃破碎紧急按钮**
					提供 1 个玻璃破碎紧急按钮，性能需满足但不限于以下内容：
					（1）紧急情况下打碎玻璃之后触发开门信号打开门禁，PC 防火阻燃材料，耐用电流 3A@36VDC。
					（2）提供三年质保服务。
		门禁卡	楚天龙	VM-IC-SSX1410	**3.9 门禁卡**
					提供 10 张门禁卡，性能需满足但不限于以下内容：
					（1）门禁卡卡内存放发行信息和卡片密钥；
					（2）门禁卡采用国家密码管理局认证的国密 CPU 卡，符合 GM/T 0028-2014《密码模块安全技术要求》（或 GB/T 37092-2018《信息安全技术密码模块安全要求》），符合 GM/T 0041-2015《智能 IC 卡密码检测规范》，安全等级第三级相关要求。
					（3）提供三年质保服务。
		后台登录读卡器	重庆中星微	VM-7816-N32	**3.10 后台登录读卡器**
					提供 1 台后台登录读卡器，性能需满足但不限于以下内容：
					（1）安全模块采用一款 32 位多用途高性能安全芯片，符合 GM/T 0008-2012《安全芯片密码检测准则》安全等级第三级相关要求；
					（2）含 5 张用户登录国密卡；
					（3）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。
					（4）提供三年质保服务。
		门禁管理后台一体机	重庆中星微	VM-ACS-YD01	**3.11 门禁管理后台一体机**
					提供 1 台门禁管理后台一体机，性能需满足但不限于以下内容：
					（1）CPU:四核；硬盘：256G SSD+1T 机械硬盘；内存：8G；
					（2）可支持 256 路门禁前端；
					（3）包含门禁管理后台软件：安装门禁管理后台软件，实现门禁设备管理、人员管理、门禁记录存储，日志管理、角色管理等功能；

					（4）后台系统与门禁前端通讯采用加密技术；
					（5）内置具有防拆功能的安全模块，安全模块应采用32位/64位多用途高性能安全芯片，且符合GM/T 0008-2012《安全芯片密码检测准则》安全等级第三级相关要求。设备密钥存储在安全芯片的密钥存储区，以此来保障服务器密钥的安全（已提供内置密码芯片经国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）；
					（6）全面符合商用密码标准，基于GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，采用经商用密码认证机构认证合格的安全芯片进行密码运算，基于杂凑算法对门禁记录定期进行完整性校验，若发现被保护数据的完整性被破坏，后台将产生告警。符合GM/T0036《采用非接触卡的门禁系统密码应用技术指南》（已提供国密安全门禁系统检测报告和国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。
					（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。
					（8）提供三年质保服务。
		硬盘	希捷	ST16000NM000J	**3.12 硬盘**
					提供2块硬盘，性能需满足但不限于以下内容：
					（1）企业级SATA硬盘
					（2）硬盘容量：16TB；
					（3）硬盘转速：7200转
					（4）提供三年质保服务。

附件二：商务条款偏离表

商务条款偏离表

采购项目编号：GXZC2025-C3-001506-HCZX

采购项目名称：广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目

分标号（此处有分标时填写具体分标号，无分标时填写“无”）：分标1

项目	磋商文件商务条款要求	供应商的承诺	偏离说明
时间和地点	合同履约期限：签订合同后90个日历日内完成项目建设实施工作，并开展初步验收，2025年11月30前申请项目竣工验收。	合同履约期限：签订合同后90个日历日内完成项目建设实施工作，并开展初步验收，2025年11月30前申请项目竣工验收。	无偏离
	服务地点：广西南宁市，锦春路3号。	服务地点：广西南宁市，锦春路3号。	无偏离
	合同签订期：自成交通知书发出之日起25日内。	合同签订期：自成交通知书发出之日起25日内。	无偏离
付款方式	合同生效后10个工作日内，采购人向成交供应商支付合同总金额50%的工程进度款；项目通过初验后，采购人向成交供应商支付支付合同总金额30%的工程进度款；项目竣工验收后采购人向成交供应商支付合同总金额20%作为合同尾款。【注：采购人付款前，成交供应商应向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至成交供应商提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一】	合同生效后10个工作日内，采购人向我公司支付合同总金额50%的工程进度款；项目通过初验后，采购人向我公司支付支付合同总金额30%的工程进度款；项目竣工验收后采购人向我公司支付合同总金额20%作为合同尾款。【注：采购人付款前，我公司应向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至我公司提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一】	无偏离
报价要求	本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。	本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。	无偏离
售后服务	1.供应商应提供技术服务热线(7*24小时)，负责解答采购人在项目执行过程中遇到的问题，并及时提出解决问题的建议和操作方法；接到采购人通知后，供应商应在30分钟内做出响应；如果需要到达现场，则供应商1小时内必须派技术人员到达现场解决问题。	1.我公司提供技术服务热线(7*24小时)，负责解答采购人在项目执行过程中遇到的问题，并及时提出解决问题的建议和操作方法；接到采购人通知后，我公司在30分钟内做出响应；如果需要到达现场，我公司1小时内派技术人员到达现场解决问题。	无偏离

	2.供应商应提供固定的售后服务和投诉渠道：固定电话热线、移动电 话热线、传真热线、电子邮箱，设定专人为本项目提供紧急维护服务。	2.我公司提供固定的售后服务和投诉渠道：固定电话热线 10009、移动电话热线：18977141161、传真热线 010-58552665、电子邮箱 18977141161@189.cn，设定专人（何江林）为本项目提供紧急维护服务。	无偏离
	3.维护期：自项目终验之日起(以验收报告的最终验收时间为准)提供至少三年免费质保。	3.维护期：自项目终验之日起（以验收报告的最终验收时间为准）提供三年免费质保，**其中对于本项目所有新购商用密码硬件产品和网络安全硬件产品（不含机房商用密码应用安全改造相关产品），提供原厂质保服务期限 6 年。**	**正偏离**
验收标准	1.项目完成全部设备上架到货、安装部署、调试、升级等工作后，方可申请初步验收。	1.项目完成全部设备上架到货、安装部署、调试、升级等工作后，方可申请初步验收。	无偏离
	2.项目完成所有建设工作后，通过网络安全等级保护测评、商用密码应用性安全评估，并取得密码管理局回函方可申请竣工验收。	2.项目完成所有建设工作后，通过网络安全等级保护测评、商用密码应用性安全评估，并取得密码管理局回函方可申请竣工验收。	无偏离
	3.验收应在采购人和供应商双方共同参加下进行。	3.验收应在采购人和我公司双方共同参加下进行。	无偏离
	4.本项目需严格按照国家相关标准、行业标准、地方标准或其他强制性标准、规范等要求进行验收。本项目如有国家相关标准、行业标准、地方标准或者其他标准、规范的，应执行相应的标准、规范。如具体采购需求与标准、规范不一致的，高于标准、规范的按具体采购需求执行，低于标准、规范的按标准、规范执行。	4.本项目需严格按照国家相关标准、行业标准、地方标准或其他强制性标准、规范等要求进行验收。本项目如有国家相关标准、行业标准、地方标准或者其他标准、规范的，应执行相应的标准、规范。如具体采购需求与标准、规范不一致的，高于标准、规范的按具体采购需求执行，低于标准、规范的按标准、规范执行。	无偏离
	5.供应商提供的应用系统密码应用适配配套设备须满足国家密码局相关要求，在项目验收中供应商提供的 IPSecVPN 安全网关须提供经国家密码管理局审批鉴定，具备商用密码产品认证，符合 GM/T 0023《IPSec VPN 网关产品规范》、GM/T 0025《SSLVPN 网关产品规范》、GM/T0026《安全 认证网关产品规范》、GM/T 0028《密码模块安全技术要求》安全等级第二级及以上要求的证书；SSL 证书须提供国家工信部颁发的电子认证服务许可证、国家密码管理局颁发的电子认证服务使用密码许可证；国密浏览器须提供具备商用密码产品认证，符合 GM/T 0028-2014《密码模块安全技术要求》安全等级第二级及以上要求	5.我公司提供的应用系统密码应用适配配套设备满足国家密码局相关要求，在项目验收中我公司提供的 IPSecVPN 安全网关须提供经国家密码管理局审批鉴定，具备商用密码产品认证，符合 GM/T 0023《IPSec VPN 网关产品规范》、GM/T 0025《SSLVPN 网关产品规范》、GM/T0026《安全 认证网关产品规范》、GM/T 0028《密码模块安全技术要求》安全等级第二级及以上要求的证书；SSL 证书提供国家工信部颁发的电子认证服务许可证、国家密码管理局颁发的电子认证服务使用密码许可证；国密浏览器提供具备商用密码产品认证，符合 GM/T 0028-2014《密码模块安全技术要求》安全等级第二级及以上要求的证书，同时提供国家信息技术安全	无偏离

	的证书，同时提供国家信息技术安全研究中心的安全性检测报告。	研究中心的安全性检测报告。	
其他要求	1.成交供应商需负责与使用部门(信息中心)的沟通对接，满足使用部门的相关合理要求。	1.我公司负责与使用部门(信息中心)的沟通对接，满足使用部门的相关合理要求。	无偏离
	2.供应商应确保所提供的产品具有合法的知识产权，如提供的产品因侵犯第三方的知识产权而引起的法律责任由供应商承担。涉及定制开发的软件系统，知识产权归采购人所有，在得到采购人书面授权前不能随意转让或授权第三方使用。软件系统所产生的数据及研究成果归采购人所有，双方均具有保密义务。	2.我公司确保所提供的产品具有合法的知识产权，如提供的产品因侵犯第三方的知识产权而引起的法律责任由我公司承担。涉及定制开发的软件系统，知识产权归采购人所有，在得到采购人书面授权前不能随意转让或授权第三方使用。软件系统所产生的数据及研究成果归采购人所有，双方均具有保密义务。	无偏离
	3.项目交付：签订合同后90个日历日内完成项目建设实施工作，并开展初步验收，2025年11月30前申请项目竣工验收。	3.项目交付：签订合同后90个日历日内完成项目建设实施工作，并开展初步验收，2025年11月30前申请项目竣工验收。	无偏离
	4.交货地点：广西南宁市，锦春路3号。	4.交货地点：广西南宁市，锦春路3号。	无偏离
	5.成交供应商与项目监理服务供应商共同完成项目档案整理与验收工作。	5.我公司与项目监理服务供应商共同完成项目档案整理与验收工作。	无偏离
	6.本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。	6.本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。	无偏离
	7.本项目所有质保服务均指原厂质保服务。	7.本项目所有质保服务均指原厂质保服务。	无偏离

附件三：技术需求偏离表

采购项目编号：GXZC2025-C3-001506-HCZX
采购项目名称：广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目
分标号（此处有分标时填写具体分标号，无分标时填写“无”）：分标 1

序号	名称	磋商文件技术需求	竞标响应	偏离说明
一	纪检监察外网商用密码应用安全改造	**1.1 安全认证网关**	**1.1 安全认证网关**	无偏离
		提供 2 台安全认证网关，性能需满足但不限于以下内容：	提供 2 台安全认证网关，性能需满足但不限于以下内容：	无偏离
		▲（1）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求，符合 GM/T 0026《安全认证网关产品规范》；（必要项）	▲（1）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求，符合 GM/T 0026《安全认证网关产品规范》；（必要项）	无偏离
		（2）设备应支持与纪检监察部门信息系统进行对接，独立完成纪检监察部门信息系统用户基于证书的身份认证和加密传输；	（2）设备应支持与纪检监察部门信息系统进行对接，独立完成纪检监察部门信息系统用户基于证书的身份认证和加密传输；	无偏离
		（3）支持办公终端防护系统通信交互，实现终端系统全方位防御互动；	（3）支持办公终端防护系统通信交互，实现终端系统全方位防御互动；	无偏离
		（4）支持纪检监察外网现有应用系统有效结合，为应用系统传递特定的数据信息；	（4）支持纪检监察外网现有应用系统有效结合，为应用系统传递特定的数据信息；**本次所有安全认证网关是我司为行业定制版本，结合中纪委身份**	正偏离

			认证体系可以实现跨省的身份互认，手持一证全国纪委行业可以实现业务认证。	
		（5）支持纪检监察外网中一次认证，跨应用、跨区域访问的单点登录功能；	（5）支持纪检监察外网中一次认证，跨应用、跨区域访问的单点登录功能；	无偏离
		（6）支持标准的协议及数据格式，可方便未来与各种系统及设备进行通信及结合；	（6）支持标准的协议及数据格式，可方便未来与各种系统及设备进行通信及结合；	无偏离
		（7）支持多种业务应用：B/S 应用、二层 C/S 应用、三层 C/S 应用等；	（7）支持多种业务应用：B/S 应用、二层 C/S 应用、三层 C/S 应用等；	无偏离
		（8）支持多证书链功能；	（8）支持多证书链功能；	无偏离
		（9）支持在线黑名单证书验证，支持海量数字证书黑名单快速检索；	（9）支持在线黑名单证书验证，支持海量数字证书黑名单快速检索；	无偏离
		▲（10）符合国家电子政务外网信任体系并通过国家电子政务外网数字证书中心的 SM2 算法的接入与应用测试；支持与纪委现有电子认证体系互信互认；	▲（10）符合国家电子政务外网信任体系并通过国家电子政务外网数字证书中心的 SM2 算法的接入与应用测试；支持与纪委现有电子认证体系互信互认；**可支持实现跨省级身份互认互信；**	**正偏离**
		（11）支持 RSA/SM2 等多种体系自适应；	（11）支持 RSA/SM2 等多种体系自适应；	无偏离
		（12）支持 SM2、SM3、SM4 等算法，具有密钥协商、身份认证、SSL 隧道加密等功能；	（12）支持 SM2、SM3、SM4 等算法，具有密钥协商、身份认证、SSL 隧道加密等功能；	无偏离
		（13）每秒新建连接数≥5000；最大并发连接数≥5000。	（13）每秒新建连接数≥5000；最大并发连接数≥**1 万**。	**正偏离**

		▲（14）安全认证网关策略统一下发系统实现客户端策略的统一下发，用户无需对客户端进行任何配置，自治区安全认证网关可以与自治区纪委从LDAP 和中纪委主 LDAP 同步证书撤销信息，验证证书有效性；	▲（14）安全认证网关策略统一下发系统实现客户端策略的统一下发，用户无需对客户端进行任何配置，自治区安全认证网关可以与自治区纪委从LDAP 和中纪委主 LDAP 同步证书撤销信息，验证证书有效性；**可支持实现跨省级 LDAP 黑名单列表信息传递；**	**正偏离**
		▲（15）提供至少三年质保服务（含软硬件）。	▲（15）提供**六年质保服务**（含软硬件）。	**正偏离**
		1.2 密码服务管理平台	**1.2 密码服务管理平台**	无偏离
		提供 1 台密码服务管理平台，性能需满足但不限于以下内容：	提供 1 台密码服务管理平台，性能需满足但不限于以下内容：	无偏离
		（1）提供一体机产品形态，支持集群化部署，满足不同场景下的部署需求，2U 机架型，≥4 个以上 RJ45 10/100/1000M 千兆网络接口；	（1）提供一体机产品形态，支持集群化部署，满足不同场景下的部署需求，2U 机架型，4 个以上 RJ45 10/100/1000M 千兆网络接口；	无偏离
		（2）支持 SM2、SM3、SM4、SM9 等商密算法；	（2）支持 SM2、SM3、SM4、SM9 等商密算法；	无偏离
		（3）支持 RSA、SHA1/SHA224/SHA256/SHA384/SHA512、3DES/AES 等通用算法；	（3）支持 RSA、SHA1/SHA224/SHA256/SHA384/SHA512、3DES/AES 等通用算法；	无偏离
		（4）支持管理的对称密钥数量：≥5000 万；	（4）支持管理的对称密钥数量：5000 万；	无偏离
		（5）支持每秒并发数≥200；	（5）支持每秒并发数 200；	无偏离
		（6）含密码计算服务、设备与服务管理服务，以及密钥管理服务；	（6）含密码计算服务、设备与服务管理服务，以及密钥管理服务；	无偏

				离
		（7）密码设备与服务管理服务：	（7）密码设备与服务管理服务：	无偏离
		1)租户管理：提供租户新增、编辑、查看、启/禁用、删除等管理功能，以及租户账户管理、授权管理等功能；	1)租户管理：提供租户新增、编辑、查看、启/禁用、删除等管理功能，以及租户账户管理、授权管理等功能；	无偏离
		2)密码服务管理：提供密码服务订阅、退订、启用/禁用、查询等管理功能，支持密码服务按需、弹性资源分配，满足动态、差异化需求，支持密码服务的扩容和变更；	2)密码服务管理：提供密码服务订阅、退订、启用/禁用、查询等管理功能，支持密码服务按需、弹性资源分配，满足动态、差异化需求，支持密码服务的扩容和变更；	无偏离
		3)应用接入管理：提供应用的新增、编辑、删除、启用/禁用、分组管理、密码服务访问授权等功能，以及通过应用认证和访问控制机制，实现对应用系统调用密码服务的统一管理和控制。（提供产品功能截图）；	3)应用接入管理：提供应用的新增、编辑、删除、启用/禁用、分组管理、密码服务访问授权等功能，以及通过应用认证和访问控制机制，实现对应用系统调用密码服务的统一管理和控制。（已提供产品功能截图）；	无偏离
		4)密码设备管理：提供对云服务器密码机、服务器密码机、时间戳服务器等密码设备的接入、使用、管控和状态监控功能，提供密码资源申请、分配、扩容等功能。提供对云服务器密码机池化管理、密码运算资源映射管理、密码资源弹性分配、密码资源智能调度功能。提供对云服务器密码机、虚拟密码机的远程升级能力。（提供产品功能截图）；	4)密码设备管理：提供对云服务器密码机、服务器密码机、时间戳服务器等密码设备的接入、使用、管控和状态监控功能，提供密码资源申请、分配、扩容等功能。提供对云服务器密码机池化管理、密码运算资源映射管理、密码资源弹性分配、密码资源智能调度功能。提供对云服务器密码机、虚拟密码机的远程升级能力。（已提供产品功能截图）；	无偏离
		5)全局监控：可以全局监控平台内所有租户应用信息，如应用名称、所属租户、状态等信息；监控服务信息，如服务在服务器节点上的分布情况、节点资源占用情况、服务状态等信息；监控设备信息，如设备资源占用情况、	5)全局监控：可以全局监控平台内所有租户应用信息，如应用名称、所属租户、状态等信息；监控服务信息，如服务在服务器节点上的分布情况、节点资源占用情况、服务状态等信息；监控设备信息，如设备资源占用情况、	无偏离

		LB/VSM 虚拟机数量、设备物理和虚拟资源状态等信息。具备告警能力和告警通知能力，提供自定义告警规则可根据提供的数据维度配置告警规则生成告警，提供告警通知规则的配置能力，支持短信、邮件等方式推送告警。支持告警转工单处理能力；	LB/VSM 虚拟机数量、设备物理和虚拟资源状态等信息。具备告警能力和告警通知能力，提供自定义告警规则可根据提供的数据维度配置告警规则生成告警，提供告警通知规则的配置能力，支持短信、邮件等方式推送告警。支持告警转工单处理能力；	
		6)统计报表：提供应用统计、密码服务统计、汇总统计三类报表，支持以租户、应用、密码服务和时间四个维度进度统计。其中应用统计支持应用分布统计、应用交易统计、应用计算接口交易排名、应用密钥使用排名。服务统计模块支持服务交易排名、服务交易结果统计、服务交易趋势、服务交易次数统计、加解密次数统计。汇总统计模块提供租户信息、服务订阅信息、租户加密、解密、签名、验签交易统计信息。（提供产品功能截图）；	6)统计报表：提供应用统计、密码服务统计、汇总统计三类报表，支持以租户、应用、密码服务和时间四个维度进度统计。其中应用统计支持应用分布统计、应用交易统计、应用计算接口交易排名、应用密钥使用排名。服务统计模块支持服务交易排名、服务交易结果统计、服务交易趋势、服务交易次数统计、加解密次数统计。汇总统计模块提供租户信息、服务订阅信息、租户加密、解密、签名、验签交易统计信息。（已提供产品功能截图）；	无偏离
		7)密码监管：提供平台整体服务、应用、密钥和密码计算规格等资源的监测，提供服务交易结果、服务资源异常、应用违规访问等维度的监测能力。提供应用合规自评估和密评风险的能力，可对应用密评合规情况进行自评和应用合规风险进行监测；	7)密码监管：提供平台整体服务、应用、密钥和密码计算规格等资源的监测，提供服务交易结果、服务资源异常、应用违规访问等维度的监测能力。提供应用合规自评估和密评风险的能力，可对应用密评合规情况进行自评和应用合规风险进行监测；	无偏离
		8)管理员管理：提供平台、租户管理员用户个人信息维护、组织机构管理、角色划分、权限划分与授权管理等功能；	8)管理员管理：提供平台、租户管理员用户个人信息维护、组织机构管理、角色划分、权限划分与授权管理等功能；	无偏离
		9)日志管理：提供对登录、操作、管理各种管理行为，以及日志备份、恢复各种日志管理的日志记录和审计功	9)日志管理：提供对登录、操作、管理各种管理行为，以及日志备份、恢复各种日志管理的日志记录和审计功	无偏离

		能。（提供产品功能截图）。	能。（已提供产品功能截图）。	
		（8）密钥管理服务：	（8）密钥管理服务：	无偏离
		1)为对称密钥、非对称密钥提供全生命周期管理服务，包括密钥生成、存储、分发、更新、备份、恢复、归档、销毁等功能；	1)为对称密钥、非对称密钥提供全生命周期管理服务，包括密钥生成、存储、分发、更新、备份、恢复、归档、销毁等功能；	无偏离
		2)支持算法：支持国密对称密钥（SM1、SM4）、国密非对称密钥（SM2）、国际算法密钥（DES、AES、KDF、RSA、ECC）；	2)支持算法：支持国密对称密钥（SM1、SM4）、国密非对称密钥（SM2）、国际算法密钥（DES、AES、KDF、RSA、ECC）；	无偏离
		3)密钥安全：使用三层密钥保护体系安全存储密钥数据，保护密钥存储安全；以应用为单位，对密钥进行细粒度逻辑隔离，保障密钥获取安全；	3)密钥安全：使用三层密钥保护体系安全存储密钥数据，保护密钥存储安全；以应用为单位，对密钥进行细粒度逻辑隔离，保障密钥获取安全；	无偏离
		4)密钥更新：支持密钥定时更新、按需主动更新，支持密钥更新策略自定义，以及基于多版本机制的统一管理，保障应用的密钥使用安全，特别是当密钥超过使用期限、已泄露、怀疑密钥不安全时（提供产品功能截图）；	4)密钥更新：支持密钥定时更新、按需主动更新，支持密钥更新策略自定义，以及基于多版本机制的统一管理，保障应用的密钥使用安全，特别是当密钥超过使用期限、已泄露、怀疑密钥不安全时（已提供产品功能截图）；	无偏离
		5)密钥多版本：支持同一密钥唯一标识下密钥的多版本管理。在密钥轮换和更新场景下，无感切换和更新密钥（提供产品功能截图）；	5)密钥多版本：支持同一密钥唯一标识下密钥的多版本管理。在密钥轮换和更新场景下，无感切换和更新密钥（已提供产品功能截图）；	无偏离
		6)密钥销毁：支持实时销毁、计划销毁密钥，支持批量销毁密钥。其中计划密钥支持自定义销毁计划，以及销毁计划调整和取消。支持通过接口和管理界面进行密钥销毁管理。（提供产品功能截图）；	6)密钥销毁：支持实时销毁、计划销毁密钥，支持批量销毁密钥。其中计划密钥支持自定义销毁计划，以及销毁计划调整和取消。支持通过接口和管理界面进行密钥销毁管理。（已提供产品功能截图）；	无偏离
		7)密钥授权：支持同平台跨租户、跨应用的密钥授权，支撑不同应用之间	7)密钥授权：支持同平台跨租户、跨应用的密钥授权，支撑不同应用之间	无偏

		数据互通。密钥的获取需符合授权范围要求，防止密钥越权访问和使用。（提供产品功能截图）；	数据互通。密钥的获取需符合授权范围要求，防止密钥越权访问和使用。（已提供产品功能截图）；	离
		8)BYOK 密钥导入：支持两段式密钥导入机制，支持导入其他源产生的密钥；	8)BYOK 密钥导入：支持两段式密钥导入机制，支持导入其他源产生的密钥；	无偏离
		9)密钥安全分发：支持基于国密安全传输通道、符合国密相关要求的身份认证、密钥的机密性和完整性保护多重保护机制的密钥安全分发；	9)密钥安全分发：支持基于国密安全传输通道、符合国密相关要求的身份认证、密钥的机密性和完整性保护多重保护机制的密钥安全分发；	无偏离
		10)密钥备份与恢复：支持定期备份密钥数据，以加密文件形式存储。支持自定义密钥备份策略，支持每天、每周或固定日期备份。备份策略支持启用和禁用两种状态。支持备份密钥文件的下载与恢复；	10)密钥备份与恢复：支持定期备份密钥数据，以加密文件形式存储。支持自定义密钥备份策略，支持每天、每周或固定日期备份。备份策略支持启用和禁用两种状态。支持备份密钥文件的下载与恢复；	无偏离
		11)密钥归档：为到期或销毁的密钥提供安全归档存储服务。支持按密钥销毁时间区间批量归档，支持手动选中指定密钥归档。归档密钥以文件形式存储。支持归档文件的下载；	11)密钥归档：为到期或销毁的密钥提供安全归档存储服务。支持按密钥销毁时间区间批量归档，支持手动选中指定密钥归档。归档密钥以文件形式存储。支持归档文件的下载；	无偏离
		12)密钥模版：支持密钥模板的灵活定制，支持自动、手动创建基于模板的密钥服务，简化密钥管理和使用的流程；	12)密钥模版：支持密钥模板的灵活定制，支持自动、手动创建基于模板的密钥服务，简化密钥管理和使用的流程；	无偏离
		13)证书托管：支持产生 P10 文件。支持托管外部 X509 证书、P12 证书，支持证书的激活、下载、别名修改和详情查看。支持匹配证书内密钥的自动关联；	13)证书托管：支持产生 P10 文件。支持托管外部 X509 证书、P12 证书，支持证书的激活、下载、别名修改和详情查看。支持匹配证书内密钥的自动关联；	无偏离
		（9）含操作系统、数据库、安全容器平台等基础软件；	（9）含操作系统、数据库、安全容器平台等基础软件；	无偏离

		▲（10）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书和密码检测报告，适用于 GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（提供商用密码产品认证证书及检测报告证明材料）；	▲（10）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书和密码检测报告，适用于 GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（已提供商用密码产品认证证书及检测报告证明材料）；	无偏离
		▲（11）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书和检验检测报告（提供检测证书和检验检测报告证明材料）；	▲（11）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书和检验检测报告（已提供检测证书和检验检测报告证明材料）；	无偏离
		（12）具备全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书，支持 IPV6 协议；	（12）具备全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书，支持 IPV6 协议；	无偏离
		（13）具备 ITPTC、CMA、CNAS 中国认可检测机构出具的软件测试报告（提供测试报告证明材料）；	（13）具备 ITPTC、CMA、CNAS 中国认可检测机构出具的软件测试报告（已提供测试报告证明材料）；	无偏离
		（14）具备计算机软件著作权登记证书（提供软件著作权登记证书证明材料）；	（14）具备计算机软件著作权登记证书（已提供软件著作权登记证书证明材料）；	无偏离
		▲（15）提供至少三年质保服务（含软硬件）。	▲（15）提供**六年质保服务**（含软硬件）。	**正偏离**
		1.3 签名验签服务器	**1.3 签名验签服务器**	无偏离
		提供 2 台签名验签服务器，性能需满足但不限于以下内容：	提供 2 台签名验签服务器，性能需满足但不限于以下内容：	无偏离
		（1）标准 2U 机架型，双电源，不低于 4 个 10/100/1000M 自适应电口，可选配 2 个 10G 光口；	（1）标准 2U 机架型，双电源，4 个 10/100/1000M 自适应电口，可选配 2 个 10G 光口；	无偏离

		（2）为保护管理账号的安全，多级权限控制：支持管理员、操作员、审计员多级权限控制，保护管理账号的安全；支持管理角色登录口令的有效期控制（提供产品操作界面截图证明）；	（2）为保护管理账号的安全，多级权限控制：支持管理员、操作员、审计员多级权限控制，保护管理账号的安全；支持管理角色登录口令的有效期控制（已提供产品操作界面截图证明）；	无偏离
		（3）支持网口绑定，提高设备的服务可靠性（提供产品操作界面截图证明）；	（3）支持网口绑定，提高设备的服务可靠性（已提供产品操作界面截图证明）；	无偏离
		▲（4）为确保供应链可靠，硬件采用国产化平台，整机和关键密码部件（密码卡或SE）均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（提供资质证书证明材料）；	▲（4）为确保供应链可靠，硬件采用国产化平台，整机和关键密码部件（密码卡或SE）均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（已提供资质证书证明材料）；	无偏离
		（5）支持通过管理页面对设备进行在线升级（提供产品操作界面截图证明）；	（5）支持通过管理页面对设备进行在线升级（已提供产品操作界面截图证明）；	无偏离
		（6）支持金融机构证书414文件批量导入和管理（提供产品操作界面截图证明）；	（6）支持金融机构证书414文件批量导入和管理（已提供产品操作界面截图证明）；	无偏离
		（7）为便于证书管理，支持多机证书自动同步，方便证书管理。可设置设备同步列表，在业务系统通过接口调用导入证书时可将该证书自动同步到其他设备（提供产品操作界面截图证明）；	（7）为便于证书管理，支持多机证书自动同步，方便证书管理。可设置设备同步列表，在业务系统通过接口调用导入证书时可将该证书自动同步到其他设备（已提供产品操作界面截图证明）；	无偏离
		（8）SM2签名/验证:≥45000/12000次/秒；	（8）SM2签名/验证:45000/12000次/秒；	无偏离
		（9）SM3:≥890Mbps；	（9）SM3:890Mbps；	无偏离
		（10）SM4加解密:≥800Mbps；	（10）SM4加解密:800Mbps；	无

				偏离
		（11）PKCS#1 签名/验证：≥28000/6500 次/秒；	（11）PKCS#1 签名/验证：28000/6500 次/秒；	无偏离
		（12）PKCS#7 签名/验证：≥5500/8500 次/秒；	（12）PKCS#7 签名/验证：5500/8500 次/秒；	无偏离
		（13）制作信封：≥890 次/秒；	（13）制作信封：890 次/秒；	无偏离
		（14）解析信封：≥1200 次/秒；	（14）解析信封：1200 次/秒；	无偏离
		（15）MTBF：≥30000 小时；	（15）MTBF：≥30000 小时；	无偏离
		▲（16）提供服务：包括设备上架安装，以及对接原数字证书认证系统，接口适配、改造等服务内容；	▲（16）提供服务：包括设备上架安装，以及对接原数字证书认证系统，接口适配、改造等服务内容；	无偏离
		▲（17）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，适用于 GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（提供商用密码产品认证证书证明材料）；	▲（17）具备国家密码管理局商用密码检测中心颁发的商用密码产品认证证书，适用于 GM/T 0028《密码模块安全技术要求》的产品安全等级要求二级（已提供商用密码产品认证证书证明材料）；	无偏离
		▲（18）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书（提供检测证书证明材料）；	▲（18）具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书（已提供检测证书证明材料）；	无偏离
		（20）具备全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书，支持 IPV6 协议；	（20）具备全球 IPv6 论坛 IPv6 Ready Logo 委员会颁发的 IPv6 Ready Logo 认证证书，支持 IPV6 协议；	无偏离
		（21）具备计算机软件著作权登记证	（21）具备计算机软件著作权登记证	无

		书（提供软件著作权登记证书证明材料）；	书（已提供软件著作权登记证书证明材料）；	偏离
		▲（22）能够与广西纪检监察外网部署的原服务器密码设备实现集群部署及对接相关工作，与中央纪检监察外网所部署服务器密码设备实现对接相关工作；	▲（22）能够与广西纪检监察外网部署的原服务器密码设备实现集群部署及对接相关工作，与中央纪检监察外网所部署服务器密码设备实现对接相关工作；	无偏离
		▲（23）提供至少三年质保服务（含软硬件）。	▲（23）提供**六年质保服务**（含软硬件）。	**正偏离**
		1.4 云服务器密码机	**1.4 云服务器密码机**	无偏离
		提供 2 台云服务器密码机，性能需满足但不限于以下内容：	提供 2 台云服务器密码机，性能需满足但不限于以下内容：	无偏离
		▲（1）国产化硬件平台；	▲（1）国产化硬件平台；	无偏离
		（2）2U 机架型，2 个 10G 光口、4 个 10/100/1000M 自适应电口；	（2）2U 机架型，2 个 10G 光口、4 个 10/100/1000M 自适应电口；	无偏离
		（3）支持 128 个 VSM 自动组成集群，集群内数据自动同步，各 VSM 保持状态一致，提供高可用的密码服务，保障业务的连续性（需提供具备 CNAS 资质检测机构出具的检测报告证明）；	（3）支持 128 个 VSM 自动组成集群，集群内数据自动同步，各 VSM 保持状态一致，提供高可用的密码服务，保障业务的连续性（已提供具备 CNAS 资质检测机构出具的检测报告证明）；	无偏离
		（4）集群内自动发现功能：零配置，集群内自动发现 VSM，并自动识别 VSM 的权重，简便易用（需提供具备 CNAS 资质检测机构出具的检测报告证明）；	（4）集群内自动发现功能：零配置，集群内自动发现 VSM，并自动识别 VSM 的权重，简便易用（已提供具备 CNAS 资质检测机构出具的检测报告证明）；	无偏离
		（5）自动负载均衡功能：集群内置负载均衡，根据自动发现结果，智能负载均衡（需提供具备 CNAS 资质检测机	（5）自动负载均衡功能：集群内置负载均衡，根据自动发现结果，智能负载均衡（已提供具备 CNAS 资质检测机	无偏离

		构出具的检测报告证明）；	构出具的检测报告证明）；	
		（6）弹性伸缩功能：支持单机纵向伸缩，集群横向伸缩，充分利用密码资源，便于业务扩展（需提供具备 CNAS 资质检测机构出具的检测报告证明）；	（6）弹性伸缩功能：支持单机纵向伸缩，集群横向伸缩，充分利用密码资源，便于业务扩展（已提供具备 CNAS 资质检测机构出具的检测报告证明）；	无偏离
		（7）可按需创建不同性能/功能/版本的 VSM，满足业务多样性需求（提供产品功能截图）；	（7）可按需创建不同性能/功能/版本的 VSM，满足业务多样性需求（已提供产品功能截图）；	无偏离
		（8）性能要求（提供产品功能截图或具备 CNAS 资质检测机构出具的检测报告证明）；	（8）性能要求（已提供产品功能截图或具备 CNAS 资质检测机构出具的检测报告证明）；	无偏离
		1)单台设备可创建 VSM 数量≥32 个；	1)单台设备可创建 VSM 数量 32 个；	无偏离
		2)SM1 加解密速率≥0.6 Gbps；	2)SM1 加解密速率 0.6 Gbps；	无偏离
		3)SM2 签名速率≥49,000 次/秒；	3)SM2 签名速率 49,000 次/秒；	无偏离
		4)SM2 验证速率≥38,000 次/秒；	4)SM2 验证速率 38,000 次/秒；	无偏离
		5)SM3 计算速率≥1.5 Gbps；	5)SM3 计算速率 1.5 Gbps；	无偏离
		6)SM4 加解密速率≥1.4 Gbps；	6)SM4 加解密速率 1.4 Gbps；	无偏离
		（9）支持对称算法：SM1/SM4/3DES/AES；支持非对称算法：SM2/RSA2048/RSA4096；支持杂凑算法：SM3/SHA1/SHA256/SHA512；	（9）支持对称算法：SM1/SM4/3DES/AES；支持非对称算法：SM2/RSA2048/RSA4096；支持杂凑算法：SM3/SHA1/SHA256/SHA512；	无偏离
		（10）支持 VSM 用户独立进行密钥管	（10）支持 VSM 用户独立进行密钥管	无

		理；	理；	偏离
		（11）提供对使用 VSM 的租户管理员进行智能密码钥匙+证书认证、对业务系统进行证书认证的功能；	（11）提供对使用 VSM 的租户管理员进行智能密码钥匙+证书认证、对业务系统进行证书认证的功能；	无偏离
		（12）支持不低于 7 种模式的网口绑定，提高设备的服务可靠性，绑定模式可设置（提供产品操作界面截图证明）；	（12）支持不低于 7 种模式的网口绑定，提高设备的服务可靠性，绑定模式可设置（已提供产品操作界面截图证明）；	无偏离
		（13）提供安全的远程管理功能；	（13）提供安全的远程管理功能；	无偏离
		▲（14）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求（提供商用密码产品认证证书证明材料）；	▲（14）具备商用密码产品认证证书，符合 GM/T 0028《密码模块安全技术要求》第二级要求（已提供商用密码产品认证证书证明材料）；	无偏离
		▲（15）采用硬件密码卡，整机和密码卡、管理USBKEY均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（提供硬件密码卡、整机、管理 USBKEY 商用密码产品认证证书证明材料）。	▲（15）采用硬件密码卡，整机和密码卡、管理USBKEY均由同一厂家设计、生产和制造，均具备国家密码管理局颁发的《商用密码产品认证证书》（已提供硬件密码卡、整机、管理 USBKEY 商用密码产品认证证书证明材料）。	无偏离
		▲（16）提供至少三年质保服务（含软硬件）。	▲（16）提供**六年质保服务**（含软硬件）。	**正偏离**
		▲（17）能够与中纪委服务器密码设备实现对接。	▲（17）能够与中纪委服务器密码设备实现对接。	无偏离
		1.5 文件安全存储网关	**1.5 文件安全存储网关**	无偏离
		提供 1 台文件安全存储网关，性能需满足但不限于以下内容：	提供 1 台文件安全存储网关，性能需满足但不限于以下内容：	无偏离

		▲(1)具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；	▲(1)具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；	无偏离
		（2）支持国密 SM2/3/4 算法；	（2）支持国密 SM2/3/4 算法；	无偏离
		（3）支持基于纪检监察外网商密体系零改造与安全认证设备互动；	（3）支持基于纪检监察外网商密体系零改造与安全认证设备互动；	无偏离
		（4）支持为多个应用提供加密服务，且应用拥有独立的文件视图；	（4）支持为多个应用提供加密服务，且应用拥有独立的文件视图；	无偏离
		（5）支持多种存储设备，包括 NFS 存储、SAN 存储、GlusterFS 等分布式存储；	（5）支持多种存储设备，包括 NFS 存储、SAN 存储、GlusterFS 等分布式存储；	无偏离
		（6）支持为非结构化文件数据（文本文件/办公文件/音视频文件/图形图像文件）、半结构化数据（XML 文件）、结构化文件数据（数据库）提供存储加密服务；	（6）支持为非结构化文件数据（文本文件/办公文件/音视频文件/图形图像文件）、半结构化数据（XML 文件）、结构化文件数据（数据库）提供存储加密服务；	无偏离
		（7）支持多种部署模式，单节点、双机热备、双活和集群部署；	（7）支持多种部署模式，单节点、双机热备、双活和集群部署；	无偏离
		（8）支持文件以密文形态进行备份和恢复，支持全量备份和增量备份，支持为不同资源定制备份策略；	（8）支持文件以密文形态进行备份和恢复，支持全量备份和增量备份，支持为不同资源定制备份策略；	无偏离
		（9）支持兼容多种密码设备，包括加密卡、密码机、云密码机、KMS 密钥管理系统等；	（9）支持兼容多种密码设备，包括加密卡、密码机、云密码机、KMS 密钥管理系统等；	无偏离
		（10）支持一文一密钥加密；	（10）支持一文一密钥加密；	无偏离

		（11）使用国密算法对非结构化数据进行加/解密运算，实现数据在存储过程中的机密性保护，SM4 加密 128KB 数据运算平均速率≥1500Mbps，SM4 解密 128KB 数据运算平均速率≥1500Mbps；	（11）使用国密算法对非结构化数据进行加/解密运算，实现数据在存储过程中的机密性保护，SM4 加密 128KB 数据运算平均速率≥1500Mbps，SM4 解密 128KB 数据运算平均速率≥1500Mbps；	无偏离
		▲（12）提供设备的上架、安装调试，文件服务器的对接适配服务；	▲（12）提供设备的上架、安装调试，文件服务器的对接适配服务；	无偏离
		▲（13）提供至少三年质保服务（含软硬件）。	▲（13）提供**六年质保服务**（含软硬件）。	**正偏离**
		1.6 数据库加密网关	**1.6 数据库加密网关**	无偏离
		提供 1 台数据库加密网关，性能需满足但不限于以下内容：	提供 1 台数据库加密网关，性能需满足但不限于以下内容：	无偏离
		▲(1)具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；	▲(1)具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）；	无偏离
		▲（2）支持纪检监察外网应用系统免改造加密，支持与文件安全存储网关联动实现数据加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数据管理；提供灵活的加密状态和非加密状态的双向转换；	▲（2）支持纪检监察外网应用系统免改造加密，支持与文件安全存储网关联动实现数据加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数据管理；提供灵活的加密状态和非加密状态的双向转换；	无偏离
		（3）支持对姓名、身份证、手机号码等密文数据进行模糊查询；	（3）支持对姓名、身份证、手机号码等密文数据进行模糊查询；	无偏离
		（4）提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次性加密进行加密，加密初始化时使	（4）提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次性加密进行加密，加密初始化时使	无偏离

		用与字段加密配置一样的加密算法和密钥；	用与字段加密配置一样的加密算法和密钥；	
		（5）支持对接入的应用系统进行访问控制，只对授权访问的应用系统提供加解密服务；	（5）支持对接入的应用系统进行访问控制，只对授权访问的应用系统提供加解密服务；	无偏离
		（6）系统可以对数据字段项设置加密规则，提供数据库列级加密，并支持对不同字段列设置不同的密钥和加密算法；	（6）系统可以对数据字段项设置加密规则，提供数据库列级加密，并支持对不同字段列设置不同的密钥和加密算法；	无偏离
		（7）系统支持 Mysql、Oracle、Sql Server、postgresql、达梦、人大金仓、oceanbase、阿里 rds、华为高斯等多种数据库；	（7）系统支持 Mysql、Oracle、Sql Server、postgresql、达梦、人大金仓、oceanbase、阿里 rds、华为高斯等多种数据库；	无偏离
		（8）支持加解密速率≥5000 单元格/秒，至少支持千万级表；	（8）支持加解密速率≥**5600** 单元格/秒，支持千万级表；	**正偏离**
		▲（9）提供设备的上架、安装调试，数据库服务器的对接适配服务；	▲（9）提供设备的上架、安装调试，数据库服务器的对接适配服务；	无偏离
		▲（10）提供至少三年质保服务（含软硬件）。	▲（10）提供**六年质保服务（含软硬件）。**	**正偏离**
		1.7 目录服务系统	**1.7 目录服务系统**	无偏离
		提供 1 套目录服务系统，性能需满足但不限于以下内容：	提供 1 套目录服务系统，性能需满足但不限于以下内容：	无偏离
		▲（1）支持 5000 及以上的条目数据；支持精确查询；支持≥2500 次/秒（≥50 线程精确查询）；	▲（1）支持 5000 及以上的条目数据，**单个目录服务系统可管理亿级条目；支持精确查询；50 线程，精确查询>10000 次/秒；**	**正偏离**
		▲（2）提供系统的安装调试以及与广西纪检监察外网部署的原数字证书系	▲（2）提供系统的安装调试以及与广西纪检监察外网部署的原数字证书系	无偏

		统对接适配等服务；	统对接适配等服务；	离
		（3）支持 LDAPV2、V3 标准，包括 RFC2251、RFC2253、RFC2254、RFC2255 及 RFC2256，支持标准的 LDIF 格式；	（3）支持 LDAPV2、V3 标准，包括 RFC2251、RFC2253、RFC2254、RFC2255 及 RFC2256，支持标准的 LDIF 格式；	无偏离
		（4）提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力；	（4）提供基于 Java 和 C 的 API 接口，具备良好的二次开发能力和整合能力；	无偏离
		（5）支持 PKI 的相关标准，支持 X.509V3 标准，支持 RFC2459、RFC2587 及 RFC3280。	（5）支持 PKI 的相关标准，支持 X.509V3 标准，支持 RFC2459、RFC2587 及 RFC3280。	无偏离
		▲（6）提供至少三年质保服务（含软硬件）。	▲（6）提供三年质保服务（含软硬件）。	无偏离
		1.8 国密浏览器	**1.8 国密浏览器**	无偏离
		提供 20 个国密浏览器授权，性能需满足但不限于以下内容：	提供 20 个国密浏览器授权，性能需满足但不限于以下内容：	无偏离
		（1）可支持国密应用识别、国密网站标识、国密根证书内置、SSL 双向通信国密加密等功能，实现采用国密算法（SM2、SM3、SM4）应用的网页访问及交互；	（1）可支持国密应用识别、国密网站标识、国密根证书内置、SSL 双向通信国密加密等功能，实现采用国密算法（SM2、SM3、SM4）应用的网页访问及交互；	无偏离
		（2）提供软件的安装，终端智能密码钥匙的适配服务；	（2）提供软件的安装，终端智能密码钥匙的适配服务；	无偏离
		▲（3）具备国家密码局商用密码检测中心颁发的浏览器密码模块商用密码产品认证证书；	▲（3）具备国家密码局商用密码检测中心颁发的浏览器密码模块商用密码产品认证证书；	无偏离
		（4）支持 HTML 和 CSS 解析，支持 JavaScrip 引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能。	（4）支持 HTML 和 CSS 解析，支持 JavaScrip 引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能。	无偏离
		▲（5）提供至少三年质保服务。	▲（5）提供三年质保服务。	无

				偏离
		1.9 智能密码钥匙	**1.9 智能密码钥匙**	无偏离
		提供 5000 个智能密码钥匙，性能需满足但不限于以下内容：	提供 5000 个智能密码钥匙，性能需满足但不限于以下内容：	无偏离
		（1）支持 SM2、SM3、SM4 算法，具有身份认证、加/解密、签名/验签等功能；	（1）支持 SM2、SM3、SM4 算法，具有身份认证、加/解密、签名/验签等功能；	无偏离
		（2）提供与原数字证书系统的对接适配，证书在线申请、导入导出等服务；	（2）提供与原数字证书系统的对接适配，证书在线申请、导入导出等服务；	无偏离
		（3）用户空间不少于 70K，数据存储年限不少于 10 年；	（3）用户空间**不少于 80K**，数据存储年限不少于 10 年；	**正偏离**
		（4）符合 CE 和 FCC 标准；遵循《智能 IC 卡及智能密码钥匙密码应用接口规范》，MS CAPI，X.509 v3 证书存储，SSL v3，IPSec，兼容 ISO 7816；	（4）符合 CE 和 FCC 标准；遵循《智能 IC 卡及智能密码钥匙密码应用接口规范》，MS CAPI，X.509 v3 证书存储，SSL v3，IPSec，兼容 ISO 7816；	无偏离
		▲（5）具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）。	▲（5）具有国家密码管理局颁发的《商用密码产品认证证书》（符合 GM/T 0028《密码模块安全技术要求》第二级要求）。	无偏离
		▲（6）提供至少三年质保服务。	▲（6）提供**六年质保服务**。	**正偏离**
		1.10 密码咨询及网络安全服务	**1.10 密码咨询及网络安全服务**	无偏离
		1.10.1 密码咨询服务	1.10.1 密码咨询服务	无偏离

		1.10.1.1 服务内容	1.10.1.1 服务内容	无偏离
		密码政策与标准咨询：国家对密码管理出台了多项法律法规，如《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等。通过该服务，对这些法律法规进行深入解析，帮助准确理解密码政策的核心要求，从而确保其在系统设计、运营和维护中保持合规。	密码政策与标准咨询：国家对密码管理出台了多项法律法规，如《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等。通过该服务，对这些法律法规进行深入解析，帮助准确理解密码政策的核心要求，从而确保其在系统设计、运营和维护中保持合规。	无偏离
		应用系统开发改造对接：根据现有系统架构，设计密码应用的对接方案，确保新密码系统与原有系统的兼容性。	应用系统开发改造对接：根据现有系统架构，设计密码应用的对接方案，确保新密码系统与原有系统的兼容性。	无偏离
		密码系统评估与优化：对现有的密码系统进行全面的安全预评估，确保系统在安全性、可用性、合规性等方面满足要求。	密码系统评估与优化：对现有的密码系统进行全面的安全预评估，确保系统在安全性、可用性、合规性等方面满足要求。	无偏离
		密码技术培训与指导：为技术团队提供密码技术的基础培训，确保被培训人员能够理解和掌握密码系统的核心概念和技术操作。	密码技术培训与指导：为技术团队提供密码技术的基础培训，确保被培训人员能够理解和掌握密码系统的核心概念和技术操作。	无偏离
		1.10.1.2 服务范围	1.10.1.2 服务范围	无偏离
		密码咨询服务将帮助自治区纪委监委优化现有密码技术体系、密码管理体系，确保单位内的相关应用系统密码应用的合规性、有效性、正确性。	密码咨询服务将帮助自治区纪委监委优化现有密码技术体系、密码管理体系，确保单位内的相关应用系统密码应用的合规性、有效性、正确性。	无偏离
		1.10.1.3 服务频率	1.10.1.3 服务频率	无偏离
		项目期内提供 1 次。	项目期内提供 1 次。	无

				偏离
		1.10.1.4 服务交付物	1.10.1.4 服务交付物	无偏离
		《政策解读与标准对接报告》、《密码应用方案设计文档》、《应用系统改造对接文档》、《码系统评估与优化报告》、《密码技术培训资料》等。	《政策解读与标准对接报告》、《密码应用方案设计文档》、《应用系统改造对接文档》、《码系统评估与优化报告》、《密码技术培训资料》等。	无偏离
		1.10.2 安全漏洞扫描服务	1.10.2 安全漏洞扫描服务	无偏离
		1.10.2.1 服务内容	1.10.2.1 服务内容	无偏离
		主要是通过安全评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，查找 WEB 应用系统、服务器主机、数据库等安全对象目标存在的安全风险、漏洞和威胁。	主要是通过安全评估工具以本地扫描的方式对评估范围内的系统和网络进行安全扫描，查找 WEB 应用系统、服务器主机、数据库等安全对象目标存在的安全风险、漏洞和威胁。	无偏离
		1.10.2.2 服务范围	1.10.2.2 服务范围	无偏离
		对单位已授权的网络安全设备、操作系统、数据库、中间件和 WEB 应用系统进行漏洞扫描。	对单位已授权的网络安全设备、操作系统、数据库、中间件和 WEB 应用系统进行漏洞扫描。	无偏离
		1.10.2.3 服务频率	1.10.2.3 服务频率	无偏离
		项目周期内提供 2 次漏洞扫描服务。	项目周期内提供 2 次漏洞扫描服务。	无偏离
		1.10.2.4 服务交付物	1.10.2.4 服务交付物	无偏

				离
		《漏洞扫描工作方案》、《漏洞扫描授权书》、《安全测试授权函》、《漏洞扫描报告》、《漏洞风险跟踪台账》等。	《漏洞扫描工作方案》、《漏洞扫描授权书》、《安全测试授权函》、《漏洞扫描报告》、《漏洞风险跟踪台账》等。	无偏离
		1.10.3 风险评估服务	1.10.3 风险评估服务	无偏离
		1.10.3.1 服务内容	1.10.3.1 服务内容	无偏离
		通过风险评估服务，全面、准确的了解被评估信息系统的安全现状、发现系统可能会出现的安全问题，保证系统处于一个高度可信任的状态。在等级保护测评工作的基础上，针对测评对象实施网络安全风险评估服务，以测评发现的技术与管理结果作为风险评估服务输入，结合风险评估标准化流程开展网络安全风险评估服务工作。主要包括如下内容：	通过风险评估服务，全面、准确的了解被评估信息系统的安全现状、发现系统可能会出现的安全问题，保证系统处于一个高度可信任的状态。在等级保护测评工作的基础上，针对测评对象实施网络安全风险评估服务，以测评发现的技术与管理结果作为风险评估服务输入，结合风险评估标准化流程开展网络安全风险评估服务工作。主要包括如下内容：	无偏离
		1.10.3.1.1 资产识别及赋值	1.10.3.1.1 资产识别及赋值	无偏离
		进行资产识别及赋值，确定组织和信息系统中的资产，明确资产价值以及相应的保密性、完整性、可用性等安全属性情况，连接资产之间的相互关系和影响，识别出重要资产，进行赋值与计算生成《资产价值分析报告》。	进行资产识别及赋值，确定组织和信息系统中的资产，明确资产价值以及相应的保密性、完整性、可用性等安全属性情况，连接资产之间的相互关系和影响，识别出重要资产，进行赋值与计算生成《资产价值分析报告》。	无偏离
		1.10.3.1.2 威胁识别及赋值	1.10.3.1.2 威胁识别及赋值	无偏离
		进行威胁识别及赋值，明确存在的威	进行威胁识别及赋值，明确存在的威	无

		胁及其发生的可能性，以及严重威胁说明，生成《威胁分析报告》。脆弱性识别及赋值	胁及其发生的可能性，以及严重威胁说明，生成《威胁分析报告》。脆弱性识别及赋值	偏离
		进行脆弱性识别及赋值，脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性涉及安全组织、安全策略、安全制度、人员安全、系统运维等方面的安全问题。根据脆弱性被威胁利用所产生的后果对脆弱性进行赋值分析，生成《安全技术脆弱性分析报告》和《安全管理脆弱性分析报告》。	进行脆弱性识别及赋值，脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性涉及安全组织、安全策略、安全制度、人员安全、系统运维等方面的安全问题。根据脆弱性被威胁利用所产生的后果对脆弱性进行赋值分析，生成《安全技术脆弱性分析报告》和《安全管理脆弱性分析报告》。	无偏离
		1.10.3.1.3 现有安全控制措施分析	1.10.3.1.3 现有安全控制措施分析	无偏离
		分析组织或信息系统已部署安全措施的有效性，包括技术和管理两方面的安全管控分析，生成《已有安全措施分析报告》。	分析组织或信息系统已部署安全措施的有效性，包括技术和管理两方面的安全管控分析，生成《已有安全措施分析报告》。	无偏离
		1.10.3.1.4 风险分析	1.10.3.1.4 风险分析	无偏离
		在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，对资产、威胁、脆弱性等评估数据进行关联计算、分析评价，生成《风险评估报告》。	在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，对资产、威胁、脆弱性等评估数据进行关联计算、分析评价，生成《风险评估报告》。	无偏离
		1.10.3.2 服务范围	1.10.3.2 服务范围	无偏离
		通过前期调研问询确定风险评估范围为：应用系统所涉及的服务器（应用以及数据库）、中间件、数据库、数	通过前期调研问询确定风险评估范围为：应用系统所涉及的服务器（应用以及数据库）、中间件、数据库、数	无偏离

		据资产以及相关管理人员、网络防护设备以及安全管理制度。	据资产以及相关管理人员、网络防护设备以及安全管理制度。	
		1.10.3.3 服务频率	1.10.3.3 服务频率	无偏离
		项目期内提供一次。	项目期内提供一次。	无偏离
		1.10.3.4 服务交付物	1.10.3.4 服务交付物	无偏离
		《资产价值分析报告》、《安全技术脆弱性分析报告》、《安全管理脆弱性分析报告》、《已有安全措施分析报告》、《风险评估报告》等。	《资产价值分析报告》、《安全技术脆弱性分析报告》、《安全管理脆弱性分析报告》、《已有安全措施分析报告》、《风险评估报告》等。	无偏离
		1.10.4 渗透测试服务	1.10.4 渗透测试服务	无偏离
		1.10.4.1 服务内容	1.10.4.1 服务内容	无偏离
		渗透测试服务是模拟黑客的思维和攻击手法，采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试，以真实有效的发现应用系统可能存在的安全漏洞，有效帮助用户识别应用系统安全风险，提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展，主要的测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等，并指导、协助开发运维单位修复漏洞。	渗透测试服务是模拟黑客的思维和攻击手法，采用人工黑盒的方式对授权指定的应用系统进行模拟攻击测试，以真实有效的发现应用系统可能存在的安全漏洞，有效帮助用户识别应用系统安全风险，提高应用系统安全防护能力。渗透测试工作以人工渗透结合工具攻击的方式开展，主要的测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、端攻击、中间人攻击、web 脚本渗透、B/S 应用程序测试等，并指导、协助开发运维单位修复漏洞。	无偏离

		1.10.4.2 服务范围	1.10.4.2 服务范围	无偏离
		服务范围≥6 个业务系统。	服务范围≥6 个业务系统。	无偏离
		1.10.4.3 服务频率	1.10.4.3 服务频率	无偏离
		项目期内提供一次。	项目期内提供一次。	无偏离
		1.10.4.4 服务交付物	1.10.4.4 服务交付物	无偏离
		《渗透测试报告》等。	《渗透测试报告》等。	无偏离
		1.10.5 应急响应服务	1.10.5 应急响应服务	无偏离
		1.10.5.1 服务内容	1.10.5.1 服务内容	无偏离
		针对突发事件，提供网络攻击行为、网络攻击事件应急响应处置和溯源分析服务，协助分析攻击来源、分析事件原因，编制事件应急处置防守报告；根据单位环境和需求，按照桌面推演或模拟演练的方式，选定 1 个特定网络安全威胁场景，协助编制网络安全应急预案，搭建模拟场景的演练环境，协同用户编制演练脚本，并按照演练方案和演练脚本组织开展应急演练工	针对突发事件，提供网络攻击行为、网络攻击事件应急响应处置和溯源分析服务，协助分析攻击来源、分析事件原因，编制事件应急处置防守报告；根据单位环境和需求，按照桌面推演或模拟演练的方式，选定 1 个特定网络安全威胁场景，协助编制网络安全应急预案，搭建模拟场景的演练环境，协同用户编制演练脚本，并按照演练方案和演练脚本组织开展应急演练工	无偏离

		作，演练完成后，协助用户编制应急演练报告，对存在的问题指导完善应急机制和流程。	作，演练完成后，协助用户编制应急演练报告，对存在的问题指导完善应急机制和流程。	
		1.10.5.2 服务范围	1.10.5.2 服务范围	无偏离
		提供 1 个场景的应急响应服务。	提供 1 个场景的应急响应服务。	无偏离
		1.10.5.3 服务频率	1.10.5.3 服务频率	无偏离
		项目期内提供 1 次服务。	项目期内提供 1 次服务。	无偏离
		1.10.5.4 服务交付物	1.10.5.4 服务交付物	无偏离
		《应急响应（处置）报告》、《应急预案》、《应急演练方案》《应急演练报告》等。	《应急响应（处置）报告》、《应急预案》、《应急演练方案》《应急演练报告》等。	无偏离
		1.10.6 安全意识培训服务	1.10.6 安全意识培训服务	无偏离
		1.10.6.1 服务内容	1.10.6.1 服务内容	无偏离
		面向单位普通职工开展 1 次集中化的信息安全意识培训，培训内容根据单位的需求可包括网络安全法律法规解读、典型网络安全事件分析、常见网络安全风险介绍以及个人信息安全防护技巧等内容，通过培训宣讲增强全体人员的网络安全意识和防范技巧，	面向单位普通职工开展 1 次集中化的信息安全意识培训，培训内容根据单位的需求可包括网络安全法律法规解读、典型网络安全事件分析、常见网络安全风险介绍以及个人信息安全防护技巧等内容，通过培训宣讲增强全体人员的网络安全意识和防范技巧，	无偏离

		提供单位整体安全防护能力。	提供单位整体安全防护能力。	
		1.10.6.2 服务范围	1.10.6.2 服务范围	无偏离
		主要面向反腐倡廉网络信息中心、党风廉政教育中心的网络和系统相关管理人员，委机关其它人员自愿原则参加。	主要面向反腐倡廉网络信息中心、党风廉政教育中心的网络和系统相关管理人员，委机关其它人员自愿原则参加。	无偏离
		1.10.6.3 服务频率	1.10.6.3 服务频率	无偏离
		项目期内提供 1 次。	项目期内提供 1 次。	无偏离
		1.10.6.4 服务交付物	1.10.6.4 服务交付物	无偏离
		《安全培训方案》、《安全培训 PPT》、《培训签到表》等。	《安全培训方案》、《安全培训 PPT》、《培训签到表》等。	无偏离
		1.10.7 数据安全管理体系建设服务	1.10.7 数据安全管理体系建设服务	无偏离
		1.10.7.1 服务内容	1.10.7.1 服务内容	无偏离
		通过识别、评估、控制和监测数据生命周期中的各个环节，确保数据的机密性、完整性和可用性。该服务包括策略制定、流程优化、技术部署、数据分级分类、人员培训及应急响应机制建立等关键要素，构建符合行业标准和法规要求的数据安全管理体系，	通过识别、评估、控制和监测数据生命周期中的各个环节，确保数据的机密性、完整性和可用性。该服务包括策略制定、流程优化、技术部署、数据分级分类、人员培训及应急响应机制建立等关键要素，构建符合行业标准和法规要求的数据安全管理体系，	无偏离

		有效防范内外部威胁，保障业务连续性。	有效防范内外部威胁，保障业务连续性。	
		1.10.7.2 服务范围	1.10.7.2 服务范围	无偏离
		涵盖了组织建设、制度流程、技术工具以及人员能力等多个方面。	涵盖了组织建设、制度流程、技术工具以及人员能力等多个方面。	无偏离
		1.10.7.3 服务频率	1.10.7.3 服务频率	无偏离
		项目期内提供 1 次服务。	项目期内提供 1 次服务。	无偏离
		1.10.7.4 服务交付物	1.10.7.4 服务交付物	无偏离
		《数据安全管理方案》等。	《数据安全管理方案》等。	无偏离
		1.11 数据库管理系统 A	**1.11 数据库管理系统 A**	无偏离
		提供 4 套数据库管理系统，性能需满足但不限于以下内容：	提供 4 套数据库管理系统，性能需满足但不限于以下内容：	无偏离
		（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。	（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。	无偏离
		（2）支持多种云计算基础设施环境，	（2）支持多种云计算基础设施环境，	无

		支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。	支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。	偏离
		（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；	（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；	无偏离
		（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。	（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。	无偏离
		（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存储引擎表的混合查询。	（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存储引擎表的混合查询。	无偏离
		（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。	（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。	无偏离
		（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；	（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；	无偏离
		（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。	（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。	无偏离

		（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移；提供专业测评机构出具的测试报告。	（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移；已提供专业测评机构出具的测试报告。	无偏离
		（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大规模并行处理集群、读写分离集群、主备集群。	（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大规模并行处理集群、读写分离集群、主备集群。	无偏离
		（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。	（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。	无偏离
		（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，需提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	无偏离
		（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，需提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	无偏离
		（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对	（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对	无偏离

		重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。	重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。	
		（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。	（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。	无偏离
		（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。	（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。	无偏离
		（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；	（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；	无偏离
		▲（18）落盘数据的“全面加密”。无论是数据文件，还是日志文件、备份文件、导入导出文件，均支持透明的存储加密。在国产 CPU 环境下的第三方专用密码设备支持；	▲（18）落盘数据的“全面加密”。无论是数据文件，还是日志文件、备份文件、导入导出文件，均支持透明的存储加密。在国产 CPU 环境下的第三方专用密码设备支持；	无偏离
		▲（19）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，需提供专业测评机构出具的测试报告。	▲（19）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，已提供专业测评机构出具的测试报告。	无偏离
		（20）数据库具备高安全性，应提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印	（20）数据库具备高安全性，已提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印	无偏离

		件。	件。	
		▲（21）应与中央纪委统建业务应用系统适配。	▲（21）应与中央纪委统建业务应用系统适配。	无偏离
		▲（22）提供至少原厂三年质保服务。	▲（22）提供原厂三年质保服务。	无偏离
		1.12 数据库管理系统 B	**1.12 数据库管理系统 B**	无偏离
		提供 1 套数据库管理系统，且与数据库管理系统 A 异构，性能需满足但不限于以下内容：	提供 1 套数据库管理系统，且与数据库管理系统 A 异构，性能需满足但不限于以下内容：	无偏离
		（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。	（1）满足信创要求，兼容多种硬件体系，可运行于鲲鹏、海光、飞腾、龙芯、申威、兆芯等多种不同 CPU 架构的服务器设备，兼容主流 windows、Linux、麒麟、UOS、中科方德、凝思、深之度、普华、思普等多种操作系统。	无偏离
		（2）支持多种云计算基础设施环境，支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。	（2）支持多种云计算基础设施环境，支持传统的虚拟机环境部署，也支持通过 Docker 容器，或在裸金属环境下部署。	无偏离
		（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；	（3）按照 CMMI5 标准研发、发行，保障产品代码质量、成熟度及稳定性；	无偏离
		（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。	（4）兼容 Oracle 的 DBA_*、ALL_*和 USER_*开头的数据字典视图、系统包；兼容 Oracle、Mysql、SQLServer、DB2、PostgreSQL 的常用系统函数。	无偏离
		（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存	（5）提供联机交易处理（OLTP）能力，同时也具备数据仓库分析（OLAP）特性。可同时支持表级的行存、列存、和行列混合存储引擎，并支持三种存	无偏离

		储引擎表的混合查询。	储引擎表的混合查询。	
		（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。	（6）支持多种开发语言 C/C++、Python、JAVA、.Net、Go、PHP、Node.js 等。	无偏离
		（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；	（7）支持 LEN、SPACE、MEDIAN、sec_to_time、time_to_sec、FIND_IN_SET、ADD_DAYS/ADD_WEEKS、field、date_format、WEEKDAY、WEEKS_BETWEEN、TEXT_EQUAL 等函数语法；支持查询 SQL 执行计划，包括查看操作符执行的操作、每个操作符所花费的时间及返回的结果条数、执行节点字节数以及执行计划操作符耗；	无偏离
		（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。	（8）兼容多种数据库开发接口与框架，包括 DPI、OCI、OO4O、OCCI、OOPI、OTL、QT、Pro*C、Python3、django、sqlalchemy、JDBC、hibernate、.NET DATA PROVIDER、EFDmProvider、EFCore、NHibernate、DDEX 插件、ODBC 等。	无偏离
		（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移；提供专业测评机构出具的测试报告。	（9）单表支持创建 2048 列；支持分区表，包括范围分区、哈希分区、列表分区、间隔分区等；支持组合分区，如可以实现列表、范围组合分区等；支持单表分区数量为 65535 个；支持分区键包含多列，列数最多达到 16 列；支持增加、删除、合并、拆分、交换、截断、重命名等分区操作；支持分区表迁移；已提供专业测评机构出具的测试报告。	无偏离
		（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大	（10）支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、实时同步集群、大	无偏离

		规模并行处理集群、读写分离集群、主备集群。	规模并行处理集群、读写分离集群、主备集群。	
		（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。	（11）兼容多种网络协议，包括 IPV4 协议、IPV6 协议、RDMA 协议。支持 Unicode、GB18030 等常用字符集，服务器和客户端工具均支持简体中文和英文来显示输出结果和错误信息。	无偏离
		（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，需提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	（12）支持表空间自动扩展，并允许调整其扩展参数，包含支持修改扩展值：next_size 值、扩展上限，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	无偏离
		（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，需提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	（13）提供数据页级恢复功能，允许从备份中还原并恢复指定的数据页，已提供由工信部下属的专业测评机构出具的带有 CNAS 标识的测试报告。	无偏离
		（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。	（14）支持 SQL 日志记录功能，支持异步日志，SQL 日志的筛选记录机制，可根据 SQL 类型、SQL 耗时等因素组合指定日志策略，帮助系统运维人员对重点 SQL 进行监控。多日志文件支持，支持为不同用户设置不同文件，降低运维人员对日志的分析难度。	无偏离
		（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。	（15）支持行列融合存储技术，支持变更缓存、高级日志等功能实现列存高频插入效率的提升和行列自动同步机制。	无偏离
		（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。	（16）提供数据库或整个服务器的冷/热备份以及对应的还原功能。支持全库备份还原，支持 B 树/堆表等级别的备份与还原。支持备份中断机制，可根据系统负载峰谷状态随时中止或恢复备份流程。	无偏离

		（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；	（17）支持全文检索，在单表 1 亿条数据的情况下进行模糊检索，前后模糊查询的检索时间<0.7ms，前模糊查询时间<0.6ms，后模糊查询的时间<0.4ms，具备高可靠性，支持闪回、完全备份、增量备份、差异备份、归档备份功能；	无偏离
		▲（18）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，需提供专业测评机构出具的测试报告。	▲（18）支持数据迁移评估和数据比对，能够支持至少一个运行中的系统实现平滑的数据迁移而不中断业务，并且单个系统中不同类型的 SQL 语法错误为零，已提供专业测评机构出具的测试报告。	无偏离
		（19）数据库具备高安全性，应提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印件。	（19）数据库具备高安全性，已提供《信息技术产品安全分级评估证书》评估保证级 4 增强级(EAL4+)证书复印件。	无偏离
		▲（20）应与中央纪委统建业务应用系统适配。	▲（20）应与中央纪委统建业务应用系统适配。	无偏离
		▲（21）提供至少原厂三年质保服务。	▲（21）提供原厂三年质保服务。	无偏离
		1.13 数据守护集群软件	**1.13 数据守护集群软件**	无偏离
		提供 4 套数据守护集群软件，性能需满足但不限于以下内容：	提供 4 套数据守护集群软件，性能需满足但不限于以下内容：	无偏离
		为确保系统运行稳定，要求所提供集群软件和数据库管理系统 A 同一品牌；	为确保系统运行稳定，所提供集群软件和数据库管理系统 A 同一品牌；	无偏离
		▲（1）提供全功能的数据库双机热备能力，完全支持单机一致的功能，不	▲（1）提供全功能的数据库双机热备能力，完全支持单机一致的功能，不	无偏

		依赖于第三方集群组件，支持备机可读。可在不停机状态下在单机系统与主备系统间平滑变换，备机时刻保持与主机的数据同步。一旦主机发生故障，备机立刻可以自动切换成新的主机，继续提供服务，同时支持客户端透明切换。	依赖于第三方集群组件，支持备机可读。可在不停机状态下在单机系统与主备系统间平滑变换，备机时刻保持与主机的数据同步。一旦主机发生故障，备机立刻可以自动切换成新的主机，继续提供服务，同时支持客户端透明切换。	离
		（2）支持一主多备，支持同步备机和异步备机等多种方式，支持备机只读，支持备机中创建使用临时表，支持列存表。	（2）支持一主多备，支持同步备机和异步备机等多种方式，支持备机只读，支持备机中创建使用临时表，支持列存表。	无偏离
		（3）数据库集群提供负载均衡能力和故障隔离能力，可根据场景调整负载均衡策略。	（3）数据库集群提供负载均衡能力和故障隔离能力，可根据场景调整负载均衡策略。	无偏离
		（4）数据库集群提供高可用性，支持秒级的故障快速切换。	（4）数据库集群提供高可用性，支持秒级的故障快速切换。	无偏离
		▲（5）数据库集群具有可扩展性，可随着用户访问量增加，对集群进行扩容，增加节点以提高。	▲（5）数据库集群具有可扩展性，可随着用户访问量增加，对集群进行扩容，增加节点以提高。	无偏离
		▲（6）提供至少原厂三年质保服务。	▲（6）提供原厂三年质保服务。	无偏离
		1.14 中间件	**1.14 中间件**	无偏离
		提供 3 套中间件，性能需满足但不限于以下内容：	提供 3 套中间件，性能需满足但不限于以下内容：	无偏离
		（1）支持主流硬件，如 Intel、AMD、龙芯、飞腾、鲲鹏、兆芯、海光、申威等；	（1）支持主流硬件，如 Intel、AMD、龙芯、飞腾、鲲鹏、兆芯、海光、申威等；	无偏离
		（2）支持主流操作系统，如 Redhat、CentOS、Windows、中标麒麟、统信 UOS、	（2）支持主流操作系统，如 Redhat、CentOS、Windows、中标麒麟、统信 UOS、	无偏

		银河麒麟、深度、普华等；	银河麒麟、深度、普华等；	离
		（3）支持主流数据库，如 OracleDB、MySQL、GaussDB、OceanBase、达梦、金仓、神通、南大通用、瀚高等；	（3）支持主流数据库，如 OracleDB、MySQL、GaussDB、OceanBase、达梦、金仓、神通、南大通用、瀚高等；	无偏离
		（4）产品具有等保密级功能，可通过 B/S 管理控制台对应用的密级标识进行选择，密级标识应与信息主体不可分离，密级标识应不得篡改	（4）产品具有等保密级功能，可通过 B/S 管理控制台对应用的密级标识进行选择，密级标识应与信息主体不可分离，密级标识应不得篡改	无偏离
		（5）中间件产品技术成熟稳定，具有国际领先性与影响力，中间件产品应至少连续三年或以上入选 Gartner 企业级应用服务器魔力象限，提供官网截图证明材料。	（5）中间件产品技术成熟稳定，具有国际领先性与影响力，中间件产品连续四年入选 Gartner 企业级应用服务器魔力象限，已提供官网截图证明材料。	无偏离
		▲（6）产品具有访问控制功能，实现等保三员功能，系统管理、安全管理和安全审计三权分立；	▲（6）产品具有访问控制功能，实现等保三员功能，系统管理、安全管理和安全审计三权分立；	无偏离
		（7）为实现对部分老版本应用系统的兼容支持，产品需支持 JavaServer Faces（JSF）标准功能框架，且同时支持在 JSF 中，可执行动态方法，中间件产品需要提供相关的支持方法及组件模块，提供证明材料；	（7）为实现对部分老版本应用系统的兼容支持，产品需支持 JavaServer Faces（JSF）标准功能框架，且同时支持在 JSF 中，可执行动态方法，中间件产品需要提供相关的支持方法及组件模块，已提供证明材料；	无偏离
		▲（8）提供至少原厂三年质保服务。	▲（8）提供原厂三年质保服务。	无偏离
二	纪检监察外网安全系	**2.1 升级远程安全评估系统**	**2.1 升级远程安全评估系统**	无偏离
		提供 1 套远程安全评估系统的升级服务，服务需满足但不限于以下内容：	提供 1 套远程安全评估系统的升级服务，服务需满足但不限于以下内容：	无偏离
		（1）可全方位系统脆弱性发现，全面发现信息系统存在的安全漏洞、应用系统安全漏洞，检查系统存在的弱口	（1）可全方位系统脆弱性发现，全面发现信息系统存在的安全漏洞、应用系统安全漏洞，检查系统存在的弱口	无偏离

	统升级	令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。	令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告。	
		（2）能从海量数据中快速定位风险，提供仪表盘报告和分析方式，在大规模安全检查后，快速定位风险类型、区域、严重程度，根据资产重要性进行排序，可以从仪表盘报告直接定位到具体主机具体漏洞。	（2）能从海量数据中快速定位风险，提供仪表盘报告和分析方式，在大规模安全检查后，快速定位风险类型、区域、严重程度，根据资产重要性进行排序，可以从仪表盘报告直接定位到具体主机具体漏洞。	无偏离
		（3）支持检测的漏洞数大于 300000 条，兼容 CVE、CNCVE、CNNVD、CNVD 等主流标准。	（3）支持检测的漏洞数大于 300000 条，兼容 CVE、CNCVE、CNNVD、CNVD 等主流标准。	无偏离
		（4）内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持自定义扫描范围和扫描策略；	（4）内置不同的漏洞模板针对 Unix、Windows 操作系统、网络设备和防火墙等模板，同时支持自定义扫描范围和扫描策略；	无偏离
		（5）能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程中的漏报和误报。	（5）能够快速准确的识别非标准端口上的应用服务类型，并进一步进行漏洞检测，极大的避免了扫描过程中的漏报和误报。	无偏离
		（6）支持手动和自动升级。自动定时升级支持 Http 代理方式，立即升级支持一键式更新。	（6）支持手动和自动升级。自动定时升级支持 Http 代理方式，立即升级支持一键式更新。	无偏离
		（7）升级完成后的设备包含四年系统漏洞软件特征升级服务，以及四年软件升级和硬件质保服务。	（7）升级完成后的设备包含四年系统漏洞软件特征升级服务，以及四年软件升级和硬件质保服务。	无偏离
		2.2 升级安全感知系统平台	**2.2 升级安全感知系统平台**	无偏离
		提供 1 套安全感知系统平台的升级服务，服务需满足但不限于以下内容：	提供 1 套安全感知系统平台的升级服务，服务需满足但不限于以下内容：	无偏离
		（1）开启主机类资产识别模块，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基线异常、操作系统、操作	（1）开启主机类资产识别模块，能够识别资产数据来源、IP 地址、主机名、MAC 地址、基线异常、操作系统、操作	无偏离

		系统详请、主机类型、服务与端口、状态、责任人、EDR 状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP 类型、识别方式、首次发现时间等；	系统详请、主机类型、服务与端口、状态、责任人、EDR 状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP 类型、识别方式、首次发现时间等；	
		（2）开启挖矿专项检测模块，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息；	（2）开启挖矿专项检测模块，帮助更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者 IP、攻击次数、威胁情报等信息；	无偏离
		（3）开启自定义分支管理模块，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等；	（3）开启自定义分支管理模块，分支管理员具备独立的管理页面，可设置分支管理员权限，如类型、责任人、管理范围、页面权限、设备权限等；	无偏离
		（4）开启威胁定性模块，支持以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；	（4）开启威胁定性模块，支持以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它 4 个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置；	无偏离
		（5）开启责任人管理模块，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自	（5）开启责任人管理模块，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自	无偏离

		动识别资产图库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理；	动识别资产图库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理；	
		（6）开启安全态势的大屏模块，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；	（6）开启安全态势的大屏模块，帮助客户更直观的看清风险、看懂威胁，产品内置（非自定义）综合态势大屏、分支安全态势、安全事件态势、全球网络攻击态势、资产态势、重大活动网络安全指挥调度大屏、设备运行态势、外联风险监控态势等不少于 15 块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便客户结合自身业务需求进行个性化设置；	无偏离
		（7）开启弱密码扫描模块，支持 SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL 等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web 空密码等；	（7）开启弱密码扫描模块，支持 SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL 等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web 空密码等；	无偏离
		（8）开启报表分析模块，可快速生成月度、季度、年度 PPT 报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，可直接通过导出的 PPT 报告进行工作汇报，帮助用户进行高效工作，体现安全工作价值；	（8）开启报表分析模块，可快速生成月度、季度、年度 PPT 报表，包含网络安全整体解读、网络安全风险详情、告警及事件响应盘点等，可直接通过导出的 PPT 报告进行工作汇报，帮助用户进行高效工作，体现安全工作价值；	无偏离

		（9）开启联动响应模块，要求支持与同品牌防火墙、行为管理、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等；	（9）开启联动响应模块，要求支持与同品牌防火墙、行为管理、应用交付、网络控制器、端点安全管理系统等自有设备进行联动，实现效果包含联动封锁、访问控制、上网提醒、冻结账号、一键查杀等；	无偏离
		（10）支持 ATT&CK 检测模块，基于 ATT&CK 能力图谱将网络安全现状映射到模型的各个阶段，支持命中攻击技术统计展示，支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产；	（10）支持 ATT&CK 检测模块，基于 ATT&CK 能力图谱将网络安全现状映射到模型的各个阶段，支持命中攻击技术统计展示，支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产；	无偏离
		（11）支持潜伏威胁黄金眼模块，支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入 IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点；	（11）支持潜伏威胁黄金眼模块，支持可视化的形式展示威胁的影响面，通过大数据分析和关联检索技术，可清晰直观看清失陷主机对其他主机的影响，评估受损情况，方便客户快速处置。支持通过首页搜索框输入 IP/域名/URL/端口/通信对进行搜索，支持基于列表模式展示横向攻击、违规访问、风险访问、可疑行为、正常访问等详细信息，建立全方位的持续性的检测能力。支持入口点溯源功能，分析出首次失陷、疑似入口点、首次遭受攻击等信息，帮助管理人员快速找到攻击入口点；	无偏离
		（12）支持 EBA 实体行为分析模块，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常	（12）支持 EBA 实体行为分析模块，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括 DGA 解析请求、外联 C&C 服务器、异常协议利用、下载可疑文件、异常	无偏离

		横向访问等；	横向访问等；	
		▲（13）提供至少三年硬件维保、软件升级、规则库更新服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供不少于一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。	▲（13）提供三年硬件维保、软件升级、规则库更新服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。	无偏离
		2.3 升级感知系统探针	**2.3 升级感知系统探针**	无偏离
		提供 1 套安全感知系统探针的升级服务，服务需满足但不限于以下内容：	提供 1 套安全感知系统探针的升级服务，服务需满足但不限于以下内容：	无偏离
		（1）开启报文检测引擎模块,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。	（1）开启报文检测引擎模块,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。	无偏离
		（2）开启 WEB 智能检测模块，支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。	（2）开启 WEB 智能检测模块，支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式。	无偏离

		(3)开启网站攻击防御模块，支持 XSS 攻击、网页木马、网站扫描、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。	(3)开启网站攻击防御模块，支持 XSS 攻击、网页木马、网站扫描、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞、自定义 WAF 规则、WAF 云防护等网站攻击检测。	无偏离
		(4) 开启敏感信息检测模块，对敏感信息进行检测，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计 2 种方式进行命中次数统计。	(4) 开启敏感信息检测模块，对敏感信息进行检测，内置身份证、MD5、手机号码、银行卡号、邮箱等敏感信息，可自定义敏感信息检测策略选择组合的敏感信息，可基于 IP 统计和连接统计 2 种方式进行命中次数统计。	无偏离
		(5) 开启漏洞利用攻击检测模块，支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。	(5) 开启漏洞利用攻击检测模块，支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。	无偏离
		(6) 开启智能语义引擎检测模块，可针对 http 隧道、java 反序列化保护等类型进行自定义设置。	(6) 开启智能语义引擎检测模块，可针对 http 隧道、java 反序列化保护等类型进行自定义设置。	无偏离
		(7) 开启网络拓扑扫描模块，支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况；	(7) 开启网络拓扑扫描模块，支持检测出网络中的网络拓扑设备进行绘制，更多直观可视化查看网络整体情况；	无偏离
		(8) 开启弱口令检测模块，支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数；	(8) 开启弱口令检测模块，支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数；	无偏离
		(9) 开启僵尸网络检测模块，支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域	(9) 开启僵尸网络检测模块，支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域	无偏离

		名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。	名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。	
		（10）开启多种类型日志传输模式授权，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。	（10）开启多种类型日志传输模式授权，包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。	无偏离
		（11）开启暴力破解检测模块，支持 FTP、IMAP、MS Sql、Mysql、Oracle、Discuz 、 Basic Authorization 、 Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat 、 Sybase 、 Weblogic 、 Wordpress 、VNC 等 73 种协议暴力破解检测；	（11）开启暴力破解检测模块，支持 FTP、IMAP、MS Sql、Mysql、Oracle、Discuz 、 Basic Authorization 、 Glassfish、POP3、RDP、Sip 、Jboss、Redis 、Ldap 、SMTP、SSH、Telnet、Tomcat 、 Sybase 、 Weblogic 、 Wordpress 、VNC 等 73 种协议暴力破解检测；	无偏离
		（12）开启传输协议审计模块，支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。	（12）开启传输协议审计模块，支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、全流量元数据审计、数据库审计协议等。	无偏离
		（13）支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。	（13）支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。	无偏离
		（14）新增自定义应用识别规则库模块，可以通过参数的灵活设定，把关注的特殊事件作为自定义策略下发给引擎进行检测。对于网络流量的异常情况具有非常准确、有效的发现能力。	（14）新增自定义应用识别规则库模块，可以通过参数的灵活设定，把关注的特殊事件作为自定义策略下发给引擎进行检测。对于网络流量的异常情况具有非常准确、有效的发现能力。	无偏离
		▲（15）提供至少三年硬件维保、软件升级、规则库更新等服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次	▲（15）提供三年硬件维保、软件升级、规则库更新等服务，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品	无偏离

		产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供不少于一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。	更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理产品。	
		2.4升级日志审计系统	**2.4升级日志审计系统**	无偏离
		提供1套日志审计系统的升级服务，服务需满足但不限于以下内容：	提供1套日志审计系统的升级服务，服务需满足但不限于以下内容：	无偏离
		（1）系统在功能性升级增加了大数据底层架构，全面日志各类安全日志接入，包括第三方网络设备、安全设备、主机日志信息等；	（1）系统在功能性升级增加了大数据底层架构，全面日志各类安全日志接入，包括第三方网络设备、安全设备、主机日志信息等；	无偏离
		（2）升级后系统支持多维度安全风险展示，可通过系统强大的数据分析能力，进行多资产数据、安全告警数据聚合，发现潜在的安全问题，利用内置的多种分析规则，对数据进行多维度关联分析；	（2）升级后系统支持多维度安全风险展示，可通过系统强大的数据分析能力，进行多资产数据、安全告警数据聚合，发现潜在的安全问题，利用内置的多种分析规则，对数据进行多维度关联分析；	无偏离
		（3）系统升级后支持高效的全文检索引擎，支持从亿级日志信息中秒级响应检索结果，支持基于关键字、多种逻辑关系符的组合运用精确查询。	（3）系统升级后支持高效的全文检索引擎，支持从亿级日志信息中秒级响应检索结果，支持基于关键字、多种逻辑关系符的组合运用精确查询。	无偏离
		（4）提供维保设备故障应急处置预案，并按预案及时解决设备故障，保障设备的高可用性，确保设备稳定运行。	（4）提供维保设备故障应急处置预案，并按预案及时解决设备故障，保障设备的高可用性，确保设备稳定运行。	无偏离
		（5）定期远程巡检和维护，根据要求对设备进行远程巡检和预防性维护，并对巡检中发现的问题给与及时修	（5）定期远程巡检和维护，根据要求对设备进行远程巡检和预防性维护，并对巡检中发现的问题给与及时修	无偏离

		复，每年度至少提交两次书面巡检报告。	复，每年度至少提交两次书面巡检报告。	
		（6）移机技术支持服务，提供设备系统移机技术支持服务，且对设备进行安装调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的调试等。	（6）移机技术支持服务，提供设备系统移机技术支持服务，且对设备进行安装调试、参数定义、逻辑卷划分、数据迁移、相关功能软件工具安装、远程备灾方案的调试等。	无偏离
		▲（7）对日志审计系统软件进行维保升级，升级内容包括至少三年硬件质保服务及软件、特征库升级更新服务。	▲（7）对日志审计系统软件进行维保升级，升级内容包括三年硬件质保服务及软件、特征库升级更新服务。	无偏离
		2.5 升级防火墙系统	**2.5 升级防火墙系统**	无偏离
		提供 2 套防火墙系统的升级服务，服务需满足但不限于以下内容：	提供 2 套防火墙系统的升级服务，服务需满足但不限于以下内容：	无偏离
		1、升级后的系统集成防火墙、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，可实现对威胁的分析、定位、处置一体化过程。具体功能如下：	1、升级后的系统集成防火墙、防病毒、入侵防御、虚拟系统、行为管理、应用层内容安全防护、威胁情报等综合安全防御功能，可实现对威胁的分析、定位、处置一体化过程。具体功能如下：	无偏离
		（1）基础防火墙功能：支持多种形式灵活部署，具备访问控制、负载均衡、VPN、虚拟系统、高可用性等功能，并可防护扫描、泛洪、异常数据包等传统网络攻击。	（1）基础防火墙功能：支持多种形式灵活部署，具备访问控制、负载均衡、VPN、虚拟系统、高可用性等功能，并可防护扫描、泛洪、异常数据包等传统网络攻击。	无偏离
		（2）防病毒：支持对 HTTP、FTP、POP3、SMTP、IMAP、SMB、IPTUX 七种协议进行病毒查杀。	（2）防病毒：支持对 HTTP、FTP、POP3、SMTP、IMAP、SMB、IPTUX 七种协议进行病毒查杀。	无偏离
		（3）入侵防御：支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL 注入、WEB 攻击、弱口令扫描等入侵行	（3）入侵防御：支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL 注入、WEB 攻击、弱口令扫描等入侵行	无偏离

		为防御。	为防御。	
		（4）虚拟系统：支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。	（4）虚拟系统：支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。	无偏离
		（5）行为管理：支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。	（5）行为管理：支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。	无偏离
		（6）应用层内容安全防护：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。	（6）应用层内容安全防护：实现 HTTP、FTP、POP3、SMTP、IMAP 五种应用协议的双向内容传输过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义。	无偏离
		（7）威胁情报：支持本地+云端威胁情报联动能力，本地威胁情报支持手动和自动升级。	（7）威胁情报：支持本地+云端威胁情报联动能力，本地威胁情报支持手动和自动升级。	无偏离
		（8）应用识别与控制：支持精确识别≥5000 余种应用，支持应用云识别。	（8）应用识别与控制：支持精确识别 5000 余种应用，支持应用云识别。	无偏离
		（9）URL 过滤：支持手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。	（9）URL 过滤：支持手动离线或自动在线进行更新升级，支持 URL 云查询，支持云端 URL 查询分析，支持自定义 URL 过滤。	无偏离
		▲2、升级完成后的设备包含至少三年威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级、授权服务，以及至少三年软件升级和硬件质保服务。	▲2、升级完成后的设备包含三年威胁情报数据订阅服务、应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级、授权服务，以及三年软件升级和硬件质保服务。	无偏离
		2.6 升级安全准入网关	**2.6 升级安全准入网关**	无偏离
		提供 2 套安全准入网关的升级服务，服务需满足但不限于以下内容：	提供 2 套安全准入网关的升级服务，服务需满足但不限于以下内容：	无偏

				离
		（1）SSL VPN 升级模块，使原有 VPN 设备支持 SSL VPN 功能；	（1）SSL VPN 升级模块，使原有 VPN 设备支持 SSL VPN 功能；	无偏离
		（2）开通授权升级模块，提供≥205 个 SSL VPN 客户端许可；	（2）开通授权升级模块，提供 205 个 SSL VPN 客户端许可；	无偏离
		（3）支持主从认证账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定；	（3）支持主从认证账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定；	无偏离
		（4）符合国密局制定的《SSL VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4；	（4）符合国密局制定的《SSL VPN 技术规范》，支持国家商用密码算法 SM1、SM2、SM3、SM4；	无偏离
		（5）支持 WEB 转发、端口转发、全网接入模式；端口转发模式支持 TCP、UDP 协议；	（5）支持 WEB 转发、端口转发、全网接入模式；端口转发模式支持 TCP、UDP 协议；	无偏离
		（6）支持智能递推；	（6）支持智能递推；	无偏离
		（7）客户端支持主流 Windows 系统、MAC 系统、Linux 系统（含 Cent OS、Ubuntu、银河麒麟、优麒麟等）；	（7）客户端支持主流 Windows 系统、MAC 系统、Linux 系统（含 Cent OS、Ubuntu、银河麒麟、优麒麟等）；	无偏离
		（8）兼容多种类型浏览器，包括 IE6、7、8、9、10、11，Chrome、Opera 、Safari、Firefox；	（8）兼容多种类型浏览器，包括 IE6、7、8、9、10、11，Chrome、Opera 、Safari、Firefox；	无偏离
		（9）支持多线路源路返回的智能选路；	（9）支持多线路源路返回的智能选路；	无偏离
		（10）支持双机热备模式下的授权漂移，仅需采购一套接入许可；	（10）支持双机热备模式下的授权漂移，仅需采购一套接入许可；	无偏离
		（11）支持 SSL VPN 会话状态监测；	（11）支持 SSL VPN 会话状态监测；	无偏离

		（12）支持通过 WebCache 技术对 web 页面进行数据优化，支持智能压缩技术，减少不必要的数据传输；	（12）支持通过 WebCache 技术对 web 页面进行数据优化，支持智能压缩技术，减少不必要的数据传输；	无偏离
		（13）支持 HTTP401 方式、WEB 方式、密码助手方式的单点登录，用户登录 VPN 后无需二次认证，即可登录内部 B/S、C/S 应用系统，支持用户修改单点登录的账户信息；	（13）支持 HTTP401 方式、WEB 方式、密码助手方式的单点登录，用户登录 VPN 后无需二次认证，即可登录内部 B/S、C/S 应用系统，支持用户修改单点登录的账户信息；	无偏离
		（14）支持基于 Android/ IOS 平台的第三方软件开发包（SDK），用于封装第三方应用软件（APP），无需安装独立客户端，即可实现数据加密传输，业务安全接入；	（14）支持基于 Android/ IOS 平台的第三方软件开发包（SDK），用于封装第三方应用软件（APP），无需安装独立客户端，即可实现数据加密传输，业务安全接入；	无偏离
		（15）支持针对 Android 平台 APP 的 VPN SDK 自动打包；	（15）支持针对 Android 平台 APP 的 VPN SDK 自动打包；	无偏离
		（16）支持 iOS、Android 智能终端以及 Windows 系统的虚拟桌面与虚拟应用发布方式接入，实现数据不落地，有效保证数据安全；	（16）支持 iOS、Android 智能终端以及 Windows 系统的虚拟桌面与虚拟应用发布方式接入，实现数据不落地，有效保证数据安全；	无偏离
		（17）支持 iOS、Android 智能终端的全网接入模式（非 PPTP 方式）；	（17）支持 iOS、Android 智能终端的全网接入模式（非 PPTP 方式）；	无偏离
		（18）支持用户名/口令、CA 证书、指纹识别、人脸识别、USB KEY、短信认证、动态令牌、硬件特征码、图形码认证；	（18）支持用户名/口令、CA 证书、指纹识别、人脸识别、USB KEY、短信认证、动态令牌、硬件特征码、图形码认证；	无偏离
		▲（19）至少提供三年软件升级和硬件质保服务。	▲（19）提供三年软件升级和硬件质保服务。	无偏离
		2.7 升级出口 vpn	**2.7 升级出口 vpn**	无偏离
		提供 1 套出口 vpn 的升级服务，服务	提供 1 套出口 vpn 的升级服务，服务	无

		需满足但不限于以下内容：	需满足但不限于以下内容：	偏离
		（1）开启单点登录功能模块，支持移动用户登录 VPN 后再登录内部 B/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全。	（1）开启单点登录功能模块，支持移动用户登录 VPN 后再登录内部 B/S 应用系统时不需要二次重复认证。支持针对 B/S 单点登录用户名密码加密传输，保证安全。	无偏离
		（2）开启断线重连模块，防止用户误操作关闭浏览器导致 VPN 隧道断开；防止用户在无线网络环境下网络正常切换时 VPN 隧道断开；	（2）开启断线重连模块，防止用户误操作关闭浏览器导致 VPN 隧道断开；防止用户在无线网络环境下网络正常切换时 VPN 隧道断开；	无偏离
		（3）支持环境检测、自动修复模块，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。	（3）支持环境检测、自动修复模块，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响 SSL VPN 的使用，减轻运维工作。	无偏离
		（4）开启用户/用户组细粒度的权限分配模块：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。	（4）开启用户/用户组细粒度的权限分配模块：可以针对被访问资源的 IP 地址、端口、提供的服务、URL 地址等进行权限控制；针对同一 B/S 资源，可对不同用户做到细致到 URL 级别的授权。	无偏离
		（5）开启基于硬件指纹特征的认证模块，可实现用户与终端的绑定，支持终端接入审批，仅允许审批通过的终端接入 VPN；支持用户自助审批；支持设置用户可允许接入的终端数量；	（5）开启基于硬件指纹特征的认证模块，可实现用户与终端的绑定，支持终端接入审批，仅允许审批通过的终端接入 VPN；支持用户自助审批；支持设置用户可允许接入的终端数量；	无偏离
		（6）开启基于 PKI 体系的第三方 CA 进行结合认证模块 ，可根据 CA 某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表。	（6）开启基于 PKI 体系的第三方 CA 进行结合认证模块 ，可根据 CA 某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持 CRL 证书撤销列表。	无偏离

		（7）开启系统实时监控模块，图形化显示一段时间内的运行状况，可查看CPU占用率、各条线路网络吞吐量、各条线路的IP地址及发送接收流速、并发会话数、SSL并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看SSL接入用户的用户名、接入时间、接入IP、虚拟IP、认证方式等信息，并可在线中断指定用户；	（7）开启系统实时监控模块，图形化显示一段时间内的运行状况，可查看CPU占用率、各条线路网络吞吐量、各条线路的IP地址及发送接收流速、并发会话数、SSL并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看SSL接入用户的用户名、接入时间、接入IP、虚拟IP、认证方式等信息，并可在线中断指定用户；	无偏离
		（8）开启独立日志中心模块，进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆SSLVPN采用非绑定账号访问应用系统的记录 ；	（8）开启独立日志中心模块，进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆SSLVPN采用非绑定账号访问应用系统的记录 ；	无偏离
		（9）开启备份模块，支持SSLVPN配置的单独备份、恢复功能，并支持历史配置的回滚 ；	（9）开启备份模块，支持SSLVPN配置的单独备份、恢复功能，并支持历史配置的回滚 ；	无偏离
		▲（10）至少提供三年硬件维保、软件升级、规则库更新，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供不少于一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟	▲（10）提供三年硬件维保、软件升级、规则库更新，以适应不断变化的网络环境和攻击手段，保持检测的准确性和有效性；提供首次产品更新和使用培训服务，确保产品的正确配置。根据实际需求和环境特点，进行个性化的设置和调整。在更新完成后，提供一人天的设备详细使用培训，包括产品的基本功能介绍、操作指南、故障排除等，确保能够熟练操作和管理	无偏离

		练操作和管理产品。	产品。	
		2.8 新增流量采集探针	**2.8 新增流量采集探针**	无偏离
		提供 1 套流量采集探针，性能需满足但不限于以下内容：	提供 1 套流量采集探针，性能需满足但不限于以下内容：	无偏离
		（1）软硬一体化 1U 标准机架式设备，标配≥4 个千兆电口，双电源，硬盘≥2T，内存≥16G，内置沙箱≥1 个；	（1）为软硬一体化 2U 标准机架式设备，标配 4 个千兆电口和 2 个扩展槽位，双电源，硬盘 **24T**，内存 **32G**，内置沙箱 1 个；	**正偏离**
		（2）吞吐量：≥1Gbps；	（2）吞吐量：**1.5Gbps**；	**正偏离**
		（3）支持多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等，能够自动解析 DNS 响应的矿池及 IP 地址；	（3）支持多样性的挖矿检测手段，能够检测挖矿木马投递、挖矿木马横向移动行为、挖矿软件、矿池域名解析、矿池连接、矿池协议等，能够自动解析 DNS 响应的矿池及 IP 地址；	无偏离
		（4）支持 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP 等多种协议报文识别，支持≥1000 种应用识别；	（4）支持 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP 等多种协议报文识别，支持≥1000 种应用识别；	无偏离
		（5）具有文件威胁检测能力，能够准确识别≥300 种文件类型；支持恶意程序分类；针对检测出的恶意文件，能够给区分类型，如木马、勒索病毒等等；能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等；	（5）具有文件威胁检测能力，能够准确识别≥300 种文件类型；支持恶意程序分类；针对检测出的恶意文件，能够给区分类型，如木马、勒索病毒等等；能够侦测各种文件型病毒，如勒索病毒、木马、僵尸、后门等；	无偏离
		（6）支持对 Web 攻击、漏洞利用、恶意软件、隐蔽隧道、黑客工具、内网	（6）支持对 Web 攻击、漏洞利用、恶意软件、隐蔽隧道、黑客工具、内网	无偏

		安全等多种类型威胁检测；	安全等多种类型威胁检测；	离
		（7）提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持WinXP、Win2003 & 2008 & 2012 server、Win7 & Win10 等主流 Windows 平台沙箱镜像；能够集成外接沙箱分析系统，提高未知威胁分析处理能力（提供功能界面截图证明）；	（7）提供内置沙箱系统，内置沙箱允许用户导入自定义镜像，并支持WinXP、Win2003 & 2008 & 2012 server、Win7 & Win10 等主流 Windows 平台沙箱镜像；能够集成外接沙箱分析系统，提高未知威胁分析处理能力（已提供功能界面截图证明）；	无偏离
		（8）内置沙箱能够对未知漏洞利用代码和恶意程序的进程操作行为、文件操作行为、系统配置操作行为、网络通信行为、恶意未知威胁逃逸行为等进行动态分析（提供功能界面截图证明）；	（8）内置沙箱能够对未知漏洞利用代码和恶意程序的进程操作行为、文件操作行为、系统配置操作行为、网络通信行为、恶意未知威胁逃逸行为等进行动态分析（已提供功能界面截图证明）；	无偏离
		（9）支持未知威胁事件证据留存，提供样本分析报告，报告内容包括：样本基本信息、执行后行为记录、重点标注恶意行为；	（9）支持未知威胁事件证据留存，提供样本分析报告，报告内容包括：样本基本信息、执行后行为记录、重点标注恶意行为；	无偏离
		（10）支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，提高运维效率；	（10）支持按照网络攻击、挖矿、扫描、暴力破解、恶意文件、威胁情报等告警进行分类，提高运维效率；	无偏离
		（11）支持 RSA、国密 SM2 加密算法的服务器私钥导入进行加密报文的解密后检测；	（11）支持 RSA、国密 SM2 加密算法的服务器私钥导入进行加密报文的解密后检测；	无偏离
		（12）具备 DNS 协议解析功能，发现发起 DGA 域名请求的失陷主机；	（12）具备 DNS 协议解析功能，发现发起 DGA 域名请求的失陷主机；	无偏离
		（13）具备威胁情报 IOC 检测能力，威胁检测类型包括：远控、钓鱼、僵尸网络、矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、黑客工具、APT 攻击事件、流氓推广、其他恶意软件等；支持域名、URL、IP 类型的威胁情报检测，对 IP 情报可	（13）具备威胁情报 IOC 检测能力，威胁检测类型包括：远控、钓鱼、僵尸网络、矿池地址、挖矿木马、勒索软件、窃密木马、远控木马、网络蠕虫、黑客工具、APT 攻击事件、流氓推广、其他恶意软件等；支持域名、URL、IP 类型的威胁情报检测，对 IP 情报可	无偏离

		以精确到端口级别；支持和威胁情报云端联动，有效检测新威胁；	以精确到端口级别；支持和威胁情报云端联动，有效检测新威胁；	
		（14）能够对相同攻击源、攻击目标、攻击类型的事件告警进行聚合，减少不必要的重复告警；内置自动研判功能，能够对攻击方向、攻击结果进行自动判定，并在告警中展示攻击结果；	（14）能够对相同攻击源、攻击目标、攻击类型的事件告警进行聚合，减少不必要的重复告警；内置自动研判功能，能够对攻击方向、攻击结果进行自动判定，并在告警中展示攻击结果；	无偏离
		（15）支持以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载；	（15）支持以某个恶意文件为中心，溯源整个文件的流转记录，并以图形化方式展示出来，直观展示在不同时间点上该恶意文件在不同主机服务器上的传播路径，支持文件下载；	无偏离
		（16）支持通过解析流量中的IP地址、端口号和应用层协议，自动识别网络资产，包括服务器类、网络设备类、终端类资产，并能够对资产进行分组管理，编辑资产信息，包括资产名称、是否核心资产等；	（16）支持通过解析流量中的IP地址、端口号和应用层协议，自动识别网络资产，包括服务器类、网络设备类、终端类资产，并能够对资产进行分组管理，编辑资产信息，包括资产名称、是否核心资产等；	无偏离
		（17）支持自动发现存在弱密码账号的资产，展示相关资产信息、以及存在弱密码的账号、密码、协议和登录端口，能够对密码进行脱敏存储和展示；	（17）支持自动发现存在弱密码账号的资产，展示相关资产信息、以及存在弱密码的账号、密码、协议和登录端口，能够对密码进行脱敏存储和展示；	无偏离
		（18）支持大屏展示，可视化展示威胁分类统计数据、排名前五的病毒事件、失陷风险最高的TOP5主机、攻击源和攻击目标地理位置等内容；	（18）支持大屏展示，可视化展示威胁分类统计数据、排名前五的病毒事件、失陷风险最高的TOP5主机、攻击源和攻击目标地理位置等内容；	无偏离
		（19）支持预设报表，包括日报、周报、月报，并支持自定义报表生成时间；	（19）支持预设报表，包括日报、周报、月报，并支持自定义报表生成时间；	无偏离
		（20）支持日志管理，可依据受害者IP、攻击者IP、文件名称、MD5等查询条件查询日志；支持Syslog协议，可以实时传输日志到syslog服务器，	（20）支持日志管理，可依据受害者IP、攻击者IP、文件名称、MD5等查询条件查询日志；支持Syslog协议，可以实时传输日志到syslog服务器，	无偏离

		选择传输的内容类型；支持同时上传多个日志服务器；	选择传输的内容类型；支持同时上传多个日志服务器；	
		（21）为保证系统稳定性和兼容性，探针必须能够与纪检监察外网现有态势感知平台对接，满足流量采集、关联分析和溯源取证要求；	（21）为保证系统稳定性和兼容性，探针必须能够与纪检监察外网现有态势感知平台对接，满足流量采集、关联分析和溯源取证要求；	无偏离
		▲（22）提供至少三年产品及授权维保服务。	▲（22）提供**六年产品及授权维保服务。**	**正偏离**
		2.9 新增万兆防火墙	**2.9 新增万兆防火墙**	无偏离
		提供 2 套万兆防火墙，性能需满足但不限于以下内容：	提供 2 套万兆防火墙，性能需满足但不限于以下内容：	无偏离
		（1）应用层吞吐量≥18G，规格：2U，内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6 千兆电口，≥4 万兆光口 SFP+(含 4 个光模块)，并发连接数≥800 万，HTTP 新建连接数≥16 万，IPSec VPN 最大接入数≥1500；	（1）应用层吞吐量 18Gbps，规格：2U，内存大小 16G，**硬盘容量 256G SSD+4T 机械硬盘，**电源：冗余电源，接口 6 个千兆电口，4 个千兆光口 SFP，4 个万兆光口 SFP+(含 4 个万兆光模块)，并发连接数 800 万，**HTTP 新建连接数 25 万，**IPSec VPN 最大接入数 1500；	**正偏离**
		（2）具备防病毒功能模块及授权，且吞吐量性能≥4G；	（2）具备防病毒功能模块及授权，且**吞吐量性能 10G；**	**正偏离**
		（3）具备 IPS 功能模块及授权，且吞吐量性能≥4G；	（3）具备 IPS 功能模块及授权，且**吞吐量性能 12G；**	**正偏离**
		（4）具备网关杀毒功能模块及授权，且吞吐量性能≥2G；	（4）具备网关杀毒功能模块及授权，且**吞吐量性能 6G；**	**正偏离**
		（5）具备全威胁处理能力模块及授权（含应用防护功能），且吞吐量性能≥2G；	（5）具备全威胁处理能力模块及授权（含应用防护功能），且**吞吐量性能 6G；**	**正偏离**

		（6）具备 IPSec VPN 能力模块及授权，且吞吐量性能≥1G；	（6）具备 IPSec VPN 能力模块及授权，且吞吐量性能 4G（AES256）或 1G（国密 SM3/SM4）；	无偏离
		（7）能够对设备环境、基础产品信息、安全性、稳定性、硬件健康状态、平台及软件健康状态进行监测，并每季度提供巡检服务并出具巡检报告；	（7）能够对设备环境、基础产品信息、安全性、稳定性、硬件健康状态、平台及软件健康状态进行监测，并每季度提供巡检服务并出具巡检报告；	无偏离
		（8）提供 7*24 小时 400 热线优先接入权益；	（8）提供 7*24 小时 400 热线（400-818-6868）优先接入权益；	无偏离
		（9）提供用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	（9）提供用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；	无偏离
		（10）提供策略生命周期管理功能，对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；	（10）提供策略生命周期管理功能，对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理；	无偏离
		（11）提供内置漏洞规则，同时要在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，用户可以自定义 IPS 规则；	（11）提供内置漏洞规则，同时要在控制台界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，用户可以自定义 IPS 规则；	无偏离
		（12）支持对具有攻击行为的 IP 采取临时禁封和永久禁封两种处理模式，IP 临时禁封功能能与设备安全防护规则实现联动；（提供产品操作界面截图证明）	（12）支持对具有攻击行为的 IP 采取临时禁封和永久禁封两种处理模式，IP 临时禁封功能能与设备安全防护规则实现联动；（已提供产品操作界面截图证明）	无偏离
		（13）支持封堵 IP 记录数量≥5 万；	（13）支持封堵 IP 记录数量≥5 万；	无偏离

		（14）针对 http 应用攻击行为日志，支持可查看攻击请求原始报文内容，包括请求头信息及 payload 详细信息等，便于专业技术人员进行分析和研判；（提供产品操作界面截图证明）	（14）针对 http 应用攻击行为日志，支持可查看攻击请求原始报文内容，包括请求头信息及 payload 详细信息等，便于专业技术人员进行分析和研判；（已提供产品操作界面截图证明）	无偏离
		▲（12）提供至少三年硬件设备故障返厂维修服务、至少三年软件升级服务、至少三年规则库更新、至少三年病毒库更新、至少三年 URL 更新。	**▲（12）提供六年硬件设备故障返厂维修服务、三年软件升级服务、三年规则库更新、三年病毒库更新、三年 URL 更新。**	**正偏离**
三	机房商用密码应用安全改造	**3.1 安全加固网关**	**3.1 安全加固网关**	无偏离
		提供 4 套安全加固网关，性能需满足但不限于以下内容：	提供 4 套安全加固网关，性能需满足但不限于以下内容：	无偏离
		（1）摄像机接入能力支持≥1 路通用网络摄像机接入；	（1）摄像机接入能力支持≥1 路通用网络摄像机接入；	无偏离
		（2）支持摄像机接入协议包括 GB/T 28181、ONVIF、RTSP 等；	（2）支持摄像机接入协议包括 GB/T 28181、ONVIF、RTSP 等；	无偏离
		（3）支持接入视频分辨率最高≥4096x2160@30fps；	（3）支持接入视频分辨率最高 4096x2160@30fps；	无偏离
		(4)接入视频编码格式 H.264/H.265；	(4)接入视频编码格式 H.264/H.265；	无偏离
		（5）输出视频编码格式支持 GB/T 25724-2017（SVAC2）；	（5）输出视频编码格式支持 GB/T 25724-2017（SVAC2）；	无偏离
		（6）输出视频分辨率包括 1920x1080P@30fps、2560x1440@30fps 等可供选择；	（6）输出视频分辨率包括 1920x1080P@30fps、2560x1440@30fps 等可供选择；	无偏离
		（7）信息安全：支持 GB 35114（达到	（7）信息安全：支持 GB 35114（达到	无

		最高安全等级C级要求），支持视频数据签名认证和加密（投标时需提供公安部出具的检测报告证明材料复印件）；	最高安全等级C级要求），支持视频数据签名认证和加密（已提供公安部出具的检测报告证明材料复印件）；	偏离
		（8）网络接口：≥2个，RJ45 10M/100M自适应以太网口，支持物理隔离（如：1路下联网络摄像机，1路上联GB 35114平台）；	（8）网络接口：2个，RJ45 10M/100M自适应以太网口，支持物理隔离（如：1路下联网络摄像机，1路上联GB 35114平台）；	无偏离
		（9）供电：DC12V-2A；	（9）供电：DC12V-2A；	无偏离
		（10）最大功耗：12W；	（10）最大功耗：12W；	无偏离
		（11）工作温度范围：-40℃～＋70℃；	（11）工作温度范围：-40℃～＋70℃；	无偏离
		（12）工作湿度范围： 0%～90%，无冷凝；	（12）工作湿度范围： 0%～90%，无冷凝；	无偏离
		（13）提供设备的安装调试以及与原机房摄相机的线路改造服务。	（13）提供设备的安装调试以及与原机房摄相机的线路改造服务。	无偏离
		（14）提供至少三年质保服务。	（14）提供三年质保服务。	无偏离
		3.2 智能密码钥匙	**3.2 智能密码钥匙**	无偏离
		提供1个智能密码钥匙，性能需满足但不限于以下内容：	提供1个智能密码钥匙，性能需满足但不限于以下内容：	无偏离
		（1）支持与CA系统协同颁发数字证书；	（1）支持与CA系统协同颁发数字证书；	无偏

				离
		（2）非对称运算（SM2）：≥5 次/秒；	（2）非对称运算（SM2）：5 次/秒；	无偏离
		（3）支持对称运算（SM4）:≥ 20Mbps/秒；	（3）支持对称运算（SM4）：20Mbps/秒；	无偏离
		（4）可支持的操作系统：win7 32/64 位、Linux 等；	（4）可支持的操作系统：win7 32/64 位、Linux 等；	无偏离
		（5）提供与原数字证书系统的对接适配，证书导入导出等服务。	（5）提供与原数字证书系统的对接适配，证书导入导出等服务。	无偏离
		（6）提供至少三年质保服务。	（6）提供三年质保服务。	无偏离
		3.3 安全智能视频一体化服务系统	**3.3 安全智能视频一体化服务系统**	无偏离
		提供 1 套安全智能视频一体化服务系统，性能需满足但不限于以下内容：	提供 1 套安全智能视频一体化服务系统，性能需满足但不限于以下内容：	无偏离
		1、功能要求：	1、功能要求：	无偏离
		（1）视频编解码支持 SVAC2.0 国家标准，兼容支持 H.264、H.265 标准（投标时需提供检测报告证明材料）	（1）视频编解码支持 SVAC2.0 国家标准，兼容支持 H.264、H.265 标准（已提供检测报告证明材料）	无偏离
		（2）信息安全标准支持 GB35114-2017，支持视频认证和加密，达到最高安全等级 C 级要求；（投标时需提供公安部出具的检测报告证明材料复印件）	（2）信息安全标准支持 GB35114-2017，支持视频认证和加密，达到最高安全等级 C 级要求；（已提供公安部出具的检测报告证明材料复印件）	无偏离
		（3）支持 IPC 设备通过 GB/T28181 协	（3）支持 IPC 设备通过 GB/T28181 协	无

		议、ONVIF 协议联网接入	议、ONVIF 协议联网接入	偏离
		（4）支持≥8 路 GB35114 A\B\C 级前端接入	（4）支持 8 路 GB35114 A\B\C 级前端接入	无偏离
		（5）WEB 客户端实时视频浏览，支持 1、4、6、9、13、16、25 多种分屏模式下实时视频浏览	（5）WEB 客户端实时视频浏览，支持 1、4、6、9、13、16、25 多种分屏模式下实时视频浏览	无偏离
		（6）支持 WEB 客户端录像回放，多种倍速回放，支持 WEB 客户端事件查询，报警信息查询	（6）支持 WEB 客户端录像回放，多种倍速回放，支持 WEB 客户端事件查询，报警信息查询	无偏离
		（7）商密认证要求：内置 UKEY 符合安全二级及以上，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性，满足密码测评要求符合商用密码产品认证证书、并符合 GM/T0028《密码模块安全技术要求》安全等级二级及以上的相关要求、支持 GB/T 39786-2021 第三级及以上密码应用基本要求的规定。（投标时需提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。	（7）商密认证要求：内置 UKEY 符合安全二级及以上，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性，满足密码测评要求符合商用密码产品认证证书、并符合 GM/T0028《密码模块安全技术要求》安全等级二级及以上的相关要求、支持 GB/T 39786-2021 第三级及以上密码应用基本要求的规定。（已提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。	无偏离
		2、硬件参数要求：	2、硬件参数要求：	无偏离
		（1）机型：≤2U	（1）机型：2U	无偏离
		（2）盘位：≥8 盘位；	（2）盘位：8 盘位；	无偏离
		（3）接入≥32Mbps，储存≥32Mbps，转发≥16Mbps；	（3）接入 32Mbps，储存 32Mbps，转发 16Mbps；	无偏

				离
		（4）支持≥4 路录像回放（单路 4Mbps 1080P）；	（4）支持 4 路录像回放（单路 4Mbps 1080P）；	无偏离
		（5）WEB 单客户端支持≥4 路 1080P 4M 码流解码；	（5）WEB 单客户端支持 4 路 1080P 4M 码流解码；	无偏离
		（6）WEB 客户端支持 35114 验签及解密播放；	（6）WEB 客户端支持 35114 验签及解密播放；	无偏离
		（7）使用国密标准的 UKEY；	（7）使用国密标准的 UKEY；	无偏离
		（8）显示输出接口：≥1 个 VGA，≥2 个 HDMI；	（8）显示输出接口：1 个 VGA，2 个 HDMI；	无偏离
		（9）网口:≥2 个千兆网口；	（9）网口:2 个千兆网口；	无偏离
		（10）提供设备的安装调试等服务。	（10）提供设备的安装调试等服务。	无偏离
		（11）提供至少三年质保服务。	（11）提供三年质保服务。	无偏离
		3.4 安全智能人脸门禁	**3.4 安全智能人脸门禁**	无偏离
		提供 1 套安全智能人脸门禁，性能需满足但不限于以下内容：	提供 1 套安全智能人脸门禁，性能需满足但不限于以下内容：	无偏离
		（1）国密安全门禁系统完全符合 GM/T0036《采用非接触卡的门禁系统密码应用技术指南》，采用国产密码	（1）国密安全门禁系统完全符合 GM/T0036《采用非接触卡的门禁系统密码应用技术指南》，采用国产密码	无偏离

		算法对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，同时对门禁记录的完整性进行保护，可应用于等保三级（及以上）信息系统的等保、密评建设和整改需求。（投标时需提供国家密码管理局商用密码检测中心颁发的门禁系统类商用密码产品认证证书复印件）	算法对重要物理区域（如计算机集中办公区、设备机房等）出入人员的身份进行鉴别，同时对门禁记录的完整性进行保护，可应用于等保三级（及以上）信息系统的等保、密评建设和整改需求。（已提供国家密码管理局商用密码检测中心颁发的门禁系统类商用密码产品认证证书复印件）	
		（2）采用国产芯片，国密算法，保障门禁系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性要求；信息安全标准支持GB35114-2017 C级安全要求；（投标时需提供公安部出具的检测报告证明材料复印件）	（2）采用国产芯片，国密算法，保障门禁系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性要求；信息安全标准支持GB35114-2017 C级安全要求；（已提供公安部出具的检测报告证明材料复印件）	无偏离
		（3）具有抓拍功能，除了抓拍正常刷脸或者刷卡开门照片上传到后台以外，还具有陌生人抓拍预警功能；	（3）具有抓拍功能，除了抓拍正常刷脸或者刷卡开门照片上传到后台以外，还具有陌生人抓拍预警功能；	无偏离
		（4）支持人脸识别加刷卡双因子认证开门方式，保证人证合一，有效防止门禁卡被乱用或者盗用；	（4）支持人脸识别加刷卡双因子认证开门方式，保证人证合一，有效防止门禁卡被乱用或者盗用；	无偏离
		（5）内置双目近红外摄像头，基于光流分析的人脸识别技术，防止照片、视频攻击；	（5）内置双目近红外摄像头，基于光流分析的人脸识别技术，防止照片、视频攻击；	无偏离
		（6）门禁基本参数：内存≥1G，存储≥1G +16G扩展储存，验证开门方式支持刷卡、人脸识别、刷卡+人脸识别；人脸比对速度：白天＜500ms 夜间＜900ms，人脸特征值存储容量≥3000条，CPU卡存储容量≥3000条，显示屏：7寸，分辨率：1024*600，工作电压：12V±10%，工作电流≤1.5A，门锁控制方式：RS485，使用环境范围：	（6）门禁基本参数：内存1G，存储1G +16G扩展储存，验证开门方式支持刷卡、人脸识别、刷卡+人脸识别；人脸比对速度：白天＜500ms 夜间＜900ms，人脸特征值存储容量3000条，CPU卡存储容量3000条，显示屏：7寸，分辨率：1024*600，工作电压：12V±10%，工作电流1.5A，门锁控制方式：RS485，使用环境范围：	无偏离

		-10~+60℃，安装方式：壁挂。	-10~+60℃，安装方式：壁挂。	
		（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（8）提供至少三年质保服务。	（8）提供三年质保服务。	无偏离
		3.5 门禁控制器	**3.5 门禁控制器**	无偏离
		提供 1 个门禁控制器，性能需满足但不限于以下内容：	提供 1 个门禁控制器，性能需满足但不限于以下内容：	无偏离
		（1）制门锁的执行单元，内置国家密码局认证的安全芯片，采用国密算法与门禁机前端进行加密通讯；	（1）制门锁的执行单元，内置国家密码局认证的安全芯片，采用国密算法与门禁机前端进行加密通讯；	无偏离
		（2）功能：单/双门单门禁机（单向），单/双门双门禁机（双向），1 路门状态反馈，1 路报警输入，RS485 通讯方式；	（2）功能：单/双门单门禁机（单向），单/双门双门禁机（双向），1 路门状态反馈，1 路报警输入，RS485 通讯方式；	无偏离
		（3）门禁控制器包括：门禁控制模块、门禁电源、漏电开关、接地排，门禁控制器机箱；	（3）门禁控制器包括：门禁控制模块、门禁电源、漏电开关、接地排，门禁控制器机箱；	无偏离
		（4）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（4）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（5）提供至少三年质保服务。	（5）提供三年质保服务。	无偏离
		3.6 双门磁力锁	**3.6 双门磁力锁**	无偏离

		提供 1 个双门磁力锁，性能需满足但不限于以下内容：	提供 1 个双门磁力锁，性能需满足但不限于以下内容：	无偏离
		（1）双门磁力锁，DC12V，LED 指示灯，门状态反馈，适合木门，铁门，有框玻璃门等。适合标准安装，门关上后门框上有固定磁力锁的位置；	（1）双门磁力锁，DC12V，LED 指示灯，门状态反馈，适合木门，铁门，有框玻璃门等。适合标准安装，门关上后门框上有固定磁力锁的位置；	无偏离
		（2）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（2）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（3）提供至少三年质保服务。	（3）提供三年质保服务。	无偏离
		3.7 开门按钮	**3.7 开门按钮**	无偏离
		提供 1 个开门按钮，性能需满足但不限于以下内容：	提供 1 个开门按钮，性能需满足但不限于以下内容：	无偏离
		（1）出门开关，ABS 阻燃塑料，白色，螺丝固定穿墙安装或配备明装 86 底盒；	（1）出门开关，ABS 阻燃塑料，白色，螺丝固定穿墙安装或配备明装 86 底盒；	无偏离
		（2）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（2）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（3）提供至少三年质保服务。	（3）提供三年质保服务。	无偏离
		3.8 玻璃破碎紧急按钮	**3.8 玻璃破碎紧急按钮**	无偏离
		提供 1 个玻璃破碎紧急按钮，性能需满足但不限于以下内容：	提供 1 个玻璃破碎紧急按钮，性能需满足但不限于以下内容：	无偏离

		（1）紧急情况下打碎玻璃之后触发开门信号打开门禁，PC 防火阻燃材料，耐用电流 3A@36VDC。	（1）紧急情况下打碎玻璃之后触发开门信号打开门禁，PC 防火阻燃材料，耐用电流 3A@36VDC。	无偏离
		（2）提供至少三年质保服务。	（2）提供三年质保服务。	无偏离
		3.9 门禁卡	**3.9 门禁卡**	无偏离
		提供 10 张门禁卡，性能需满足但不限于以下内容：	提供 10 张门禁卡，性能需满足但不限于以下内容：	无偏离
		（1）门禁卡卡内存放发行信息和卡片密钥；	（1）门禁卡卡内存放发行信息和卡片密钥；	无偏离
		（2）门禁卡采用国家密码管理局认证的国密 CPU 卡，符合 GM/T 0028-2014《密码模块安全技术要求》（或 GB/T 37092-2018《信息安全技术密码模块安全要求》），符合 GM/T 0041-2015《智能 IC 卡密码检测规范》，安全等级第三级相关要求。	（2）门禁卡采用国家密码管理局认证的国密 CPU 卡，符合 GM/T 0028-2014《密码模块安全技术要求》（或 GB/T 37092-2018《信息安全技术密码模块安全要求》），符合 GM/T 0041-2015《智能 IC 卡密码检测规范》，安全等级第三级相关要求。	无偏离
		（3）提供至少三年质保服务。	（3）提供三年质保服务。	无偏离
		3.10 后台登录读卡器	**3.10 后台登录读卡器**	无偏离
		提供 1 台后台登录读卡器，性能需满足但不限于以下内容：	提供 1 台后台登录读卡器，性能需满足但不限于以下内容：	无偏离
		（1）安全模块采用一款 32 位多用途高性能安全芯片，符合 GM/T 0008-2012《安全芯片密码检测准则》	（1）安全模块采用一款 32 位多用途高性能安全芯片，符合 GM/T 0008-2012《安全芯片密码检测准则》	无偏离

		安全等级第三级相关要求；	安全等级第三级相关要求；	
		（2）至少含 5 张用户登录国密卡；	（2）含 5 张用户登录国密卡；	无偏离
		（3）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（3）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（4）提供至少三年质保服务。	（4）提供三年质保服务。	无偏离
		3.11 门禁管理后台一体机	**3.11 门禁管理后台一体机**	无偏离
		提供 1 台门禁管理后台一体机，性能需满足但不限于以下内容：	提供 1 台门禁管理后台一体机，性能需满足但不限于以下内容：	无偏离
		（1）CPU:≥四核；硬盘：≥256G SSD+1T 机械硬盘；内存：≥8G；	（1）CPU:四核；硬盘：256G SSD+1T 机械硬盘；内存：8G；	无偏离
		（2）可支持≥256 路门禁前端；	（2）可支持 256 路门禁前端；	无偏离
		（3）包含门禁管理后台软件：安装门禁管理后台软件，实现门禁设备管理、人员管理、门禁记录存储，日志管理、角色管理等功能；	（3）包含门禁管理后台软件：安装门禁管理后台软件，实现门禁设备管理、人员管理、门禁记录存储，日志管理、角色管理等功能；	无偏离
		（4）后台系统与门禁前端通讯采用加密技术；	（4）后台系统与门禁前端通讯采用加密技术；	无偏离
		（5）内置具有防拆功能的安全模块，安全模块应采用 32 位/64 位多用途高性能安全芯片，且符合 GM/T 0008-2012《安全芯片密码检测准则》安全等级第三级相关要求。设备密钥	（5）内置具有防拆功能的安全模块，安全模块应采用 32 位/64 位多用途高性能安全芯片，且符合 GM/T 0008-2012《安全芯片密码检测准则》安全等级第三级相关要求。设备密钥	无偏离

		存储在安全芯片的密钥存储区，以此来保障服务器密钥的安全（投标时需提供内置密码芯片经国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）；	存储在安全芯片的密钥存储区，以此来保障服务器密钥的安全（已提供内置密码芯片经国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）；	
		（6）全面符合商用密码标准，基于GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，采用经商用密码认证机构认证合格的安全芯片进行密码运算，基于杂凑算法对门禁记录定期进行完整性校验，若发现被保护数据的完整性被破坏，后台将产生告警。符合GM/T0036《采用非接触卡的门禁系统密码应用技术指南》（投标时需提供国密安全门禁系统检测报告和国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。	（6）全面符合商用密码标准，基于GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，采用经商用密码认证机构认证合格的安全芯片进行密码运算，基于杂凑算法对门禁记录定期进行完整性校验，若发现被保护数据的完整性被破坏，后台将产生告警。符合GM/T0036《采用非接触卡的门禁系统密码应用技术指南》（已提供国密安全门禁系统检测报告和国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件）。	无偏离
		（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	（7）提供原门禁系统的拆除或利旧，以及新门禁系统的综合布线等安装调试服务。	无偏离
		（8）提供至少三年质保服务。	（8）提供三年质保服务。	无偏离
		3.12 硬盘	**3.12 硬盘**	无偏离
		提供2块硬盘，性能需满足但不限于以下内容：	提供2块硬盘，性能需满足但不限于以下内容：	无偏离
		（1）企业级SATA硬盘	（1）企业级SATA硬盘	无偏离
		（2）硬盘容量：≥16TB；	（2）硬盘容量：16TB；	无

				偏离
		（3）硬盘转速：≥7200 转	（3）硬盘转速：7200 转	无偏离
		（4）提供至少三年质保服务。	（4）提供三年质保服务。	无偏离

附件四：售后服务承诺书

承诺书

致中国共产党广西壮族自治区纪律检查委员会：

我公司针对 广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目 （项目编号： GXZC2025-C3-001506-HCZX ）标项一广西纪检监察外网改造建设项目的售后服务承诺如下：

时间和地点承诺

1、合同履约期限：签订合同后 90 个日历日内完成项目建设实施工作，并开展初步验收，2025 年 11 月 30 前申请项目竣工验收。

2、服务地点：广西南宁市，锦春路 3 号。

3、合同签订期：自成交通知书发出之日起 25 日内。

付款方式承诺

合同生效后 10 个工作日内，采购人向我公司支付合同总金额 50%的工程进度款；项目通过初验后，采购人向我公司支付合同总金额 30%的工程进度款；项目竣工验收后采购人向我公司支付合同总金额 20%作为合同尾款。【注：采购人付款前，我公司向采购人开具等额有效的增值税发票，采购人未收到合格有效发票的，有权不予支付相应款项直至我公司提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一】

报价承诺

我公司对本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。

售后服务承诺

1.我公司提供技术服务热线（7*24 小时）18977141161，负责解答采购人在项目执行过程中遇到的问题，并及时提出解决问题的建议和操作方法；接到采购人通知后，我公司在 30 分钟内做出响应；如果需要到达现场，则我公司将 1 小时内必须派技术人员到达现场解决问题。

2.我公司提供固定的售后服务和投诉渠道：固定电话热线 10009、移动电话热线：18977141161、传真热线 010-58552665、电子邮箱 18977141161@189.cn，设定专人何江林为

本项目提供紧急维护服务。

3.维护期：自项目终验之日起（以验收报告的最终验收时间为准）提供三年免费质保，其中对于本项目所有新购商用密码硬件产品和网络安全硬件产品（不含机房商用密码应用安全改造相关产品），提供原厂质保服务期限 6 年。

验收承诺

1.项目完成全部设备上架到货、安装部署、调试、升级等工作后，方可申请初步验收。

2.项目完成所有建设工作后，通过网络安全等级保护测评、商用密码应用性安全评估，并取得密码管理局回函方可申请竣工验收。

3.验收应在采购人和供应商双方共同参加下进行。

4.本项目需严格按照国家相关标准、行业标准、地方标准或其他强制性标准、规范等要求进行验收。本项目如有国家相关标准、行业标准、地方标准或者其他标准、规范的，应执行相应的标准、规范。如具体采购需求与标准、规范不一致的，高于标准、规范的按具体采购需求执行，低于标准、规范的按标准、规范执行。

5.我公司提供的应用系统密码应用适配配套设备满足国家密码局相关要求，在项目验收中我公司提供的 IPSecVPN 安全网关提供经国家密码管理局审批鉴定，具备商用密码产品认证，符合 GM/T 0023《IPSec VPN 网关产品规范》、GM/T 0025《SSLVPN 网关产品规范》、GM/T0026《安全认证网关产品规范》、GM/T 0028《密码模块安全技术要求》安全等级第二级及以上要求的证书；SSL 证书须提供国家工信部颁发的电子认证服务许可证、国家密码管理局颁发的电子认证服务使用密码许可证；国密浏览器须提供具备商用密码产品认证，符合 GM/T 0028-2014《密码模块安全技术要求》安全等级第二级及以上要求的证书，同时提供国家信息技术安全研究中心的安全性检测报告。

其它承诺

1.我公司负责与使用部门（信息中心）的沟通对接，满足使用部门的相关合理要求。

2.我公司确保所提供的产品具有合法的知识产权，如提供的产品因侵犯第三方的知识产权而引起的法律责任由我公司承担。涉及定制开发的软件系统，知识产权归采购人所有，在得到采购人书面授权前不能随意转让或授权第三方使用。软件系统所产生的数据及研究成果归采购人所有，双方均具有保密义务。

3.项目交付：签订合同后 90 个日历日内完成项目建设实施工作，并开展初步验收，2025 年 11 月 30 前申请项目竣工验收。

4.交货地点：广西南宁市，锦春路 3 号。

5.我公司与项目监理服务供应商共同完成项目档案整理与验收工作。

6.本项目实行总承包报价：包括货物和服务采购、实施、验收、培训、专家评审等各种费用和售后服务、税金及其它所有成本费用的总和。采购人不再支付任何费用。

7.本项目所有质保服务均指原厂质保服务。

附件五：成交通知书

成交通知书

广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目（项目编号：GXZC2025-C3-001506-HCZX）

中电信数智科技有限公司：

你单位参加了广西纪检监察外网改造建设项目和广西纪检监察外网改造建设监理服务项目分标1广西纪检监察外网改造建设项目的磋商活动，项目编号：GXZC2025-C3-001506-HCZX，经磋商小组评定，确定你公司为本项目分标1广西纪检监察外网改造建设项目的成交人，成交金额为：人民币贰佰捌拾万元整（¥2800000.00），合同履约期限：签订合同后90个日历日内完成项目建设实施工作，并开展初步验收，2025年11月30前申请项目竣工验收。

根据竞争性磋商文件中“第二章 供应商须知 29.签订合同”：

一、成交供应商在收到成交通知书后，应当在签订合同时向采购人出示相关证明材料，具体内容详见 “供应商须知前附表”，经采购人核验合格后方可签订合同。

二、签订合同时间：成交人在领取成交通知书后十五天内签订合同。

三、成交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成交候选人名单排序，确定下一候选人为成交供应商，也可以重新开展项目采购活动。拒绝签订采购合同的成交供应商不得参加对该合同项重新开展的采购活动。

四、签订合同时请带齐下列材料：

（1）成交通知书。

（2）竞争性磋商文件规定的文件材料（含法定代表人授权委托书）。

（3）单位公章或合同专用章。

（4）本单位的开户银行、帐号及开户名称。

特此通知。

采购人：中国共产党广西壮族自治区纪律检查委员会（盖章）

采购代理机构：广西汉昌工程咨询有限公司（盖章）

2025年6月23日

附件六：授权书

中电信数智科技有限公司

授权委托书

为提高中电信数智科技有限公司参与项目投标工作的效率，实现客户项目实施及支撑的本地化，提高客户需求响应速度，现就以下事宜对中电信数智科技有限公司广西分公司进行授权委托：

1、授权中电信数智科技有限公司广西分公司代表中电信数智科技有限公司参加所有客户发起的项目招投标，并在中电信数智科技有限公司授权范围内与客户签约。

2、授权中电信数智科技有限公司广西分公司代表中电信数智科技有限公司，以中电信数智科技有限公司广西分公司名义对外签约。

3、授权中电信数智科技有限公司广西分公司负责人陈善伟在所有项目的投标、开标、评标、合同谈判及签署过程中，在中电信数智科技有限公司授权范围内代表中电信数智科技有限公司法定代表人签署文件，并派员处理与招投标项目有关的事务。

4、授权中电信数智科技有限公司广西分公司组织相关项目实施、回款及售后支撑服务工作，承担与客户合同中约定的相关工作。

5、授权中电信数智科技有限公司广西分公司在投标项目时使用中电信数智科技有限公司资质，包括但不限于信息安全服务资质、安防一级资质等。

6、本授权委托书有效期限为：自签字盖章之日起一年。

中电信数智科技有限公司（公章）

法定代表人（签字/章）

二〇二五年 三月六日