

水风光多能互补联合实验室鱼背山科研成果验证基地建设 EPC 工程总承包项目
网络安全防护设备采购（第二次）
询价文件

采 购 人 重庆长电渝电力工程有限公司

2026 年 6 月



目 录

第一章	采购公告	3
第二章	评审办法	7
第三章	合同条款及格式	11
第四章	网络安全防护设计方案	45
第五章	报价文件格式	82

第一章 采购公告

水风光多能互补联合实验室鱼背山科研成果验证基地建设 EPC 工程总承包项目网络安全防护设备（第二次）采购公告

1. 采购条件

根据我司市场承揽项目获取情况，采购人重庆长电渝电力工程有限公司（以下简称：采购人）计划对水风光多能互补联合实验室鱼背山科研成果验证基地建设 EPC 工程总承包项目网络安全防护设备（第二次）采购进行询价，本项目由采购人自主采购，项目已具备采购条件，现发布采购公告。

2. 采购范围

2.1 采购概况：

鱼背山电厂水风光多能互补联合实验室鱼背山科研成果验证基地 35kV 光伏发电系统直接接入到电网调度网络，其涉及光伏发电、能源调度、设备监控等核心业务，其网络系统承载着电站的运行数据、设备管控信息等关键内容，直接关系到调度网络的安全稳定运行以及区域能源供应的可靠性，需按国家相关要求完善网安设备配置。

2.2 采购范围和内容：

1.本次采购主要内容：完成水风光多能互补联合实验室鱼背山科研成果验证基地建设 EPC 工程总承包项目网络安全设备的供货、安装调试、网安服务工作，包括但不限于：根据网络安全防护设计方案及设备清单的要求，完成相关设备的供货；并提供必要的人力、设备及材料、工器具、试验仪器完成网络安全设备的安装调试、网安服务等工作。本项目采购的网络安全设备需满足国家网络安全等级保护二级（等保二级）要求，其具体技术参数与要求见第四章 网络安全防护设计方案。

2.3 交货、安装调试及网安服务安排：

本次拟采购设备在合同签订后 30 个日历日内交货（鱼背山水电厂水风光联合控制室室内交货），自采购人通知安装之日起 45 个日历日内完成安装调试、

网络安全服务并通过竣工验收，同时，报价人自项目验收合格当日起，提供为期 1 年的免费网络安全咨询服务，具体开工时间以采购人通知为准。

3. 报价人资格要求（以下条件需同时具备）

（1）资质条件：具有独立法人资格；

（2）业绩要求：2023 年 1 月 1 日至报价截止时间止（以合同签订时间为准），提供一个国产网络安全设备（芯片、操作系统均为国产，需要提供国产化相关证明）采购项目合同金额 40 万元以上的案例，案例要求提供合同关键页、发票（发票开具时间需早于本项目采购公告之日）等。

（3）信誉要求：未被“信用中国”“国家企业信息公示”等系统列入失信被执行人名单；

（4）其他要求：1.单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一标段投标或者未划分标段的同一招标项目报价；2.所提供的设备需要提供售后服务承诺函并加盖公章(不含通信 330 以太网板)。

采购人不接受联合体报价。

4. 报价人征集方式

本次采购采用公开征集方式确定供应商。

5. 采购文件的获取

本次询价公告在重庆三峡水利电力集团股份有限公司（<http://www.cqxsxl.com/>）网上发布，我公司对其他网站或媒体转载的公告及公告内容不承担任何责任。

6. 报价文件的递交

6.1 报价截止时间：2026 年 6 月 12 日 10 时（北京时间）。

6.2 递交方式：报价截止时间前，报价人在线递交电子版报价文件至指定邮箱：CDYQCQ2025@163.com。上传至邮箱的报价文件应一式两份，即完整签章的扫描 PDF 版和与之名称和内容完全一致的可编辑版，若两个版本内容不一致时，以 PDF 版为准。

6.3 报价文件签字或盖章要求：报价文件应按第五章“报价文件格式”进行编写，如有必要，可以增加附页，作为报价文件的组成部分，最终提交文件为签字盖章后的 PDF 版本文件。不要求每页签字、盖章，但报价文件封面、报价

函、报价文件有明确规定的地方要求企业负责人或授权委托人签字并加盖单位公章。

7. 注意事项

7.1 报价有效期：自最终报价截止之日起 90 天。

7.2 踏勘现场

不组织

7.3 最高限价

本次采购最高含税限价为 878750.00 元，超出限价视为无效报价。

7.4 履约担保

本项目成交人不提交履约担保。

8. 联系方式

采购人：重庆长电渝电力工程有限公司	采购代理：_____ / _____
地址：重庆市两江新区聚贤岩广场 6 号力帆中心 1 号楼 27-5	地址：_____ / _____
邮编：400000	邮编：_____ / _____
联系人：朱先生	联系人：_____ / _____
电话：15858189236	电话：_____ / _____
传真：_____ / _____	传真：_____ / _____
电子邮箱：CDYCQ2025@163.com	电子邮箱：_____ / _____
电话：15858189236	电话：_____ / _____
异议或投诉处理:1.报价人或者其他利害关系人就本项目的评审结果等事项提出异议或投诉的，应当先向采购人提出异议；采购人应当在规定时间内答复；对采购人的答复不满意，可向监督部门投诉。 2.监督部门依照《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》、《工程建设项目招标投标活动投诉处理办法》（七部委令第 11 号（根据九部门 2013 年第	

23 号令修正)) 等法律法规文件处理投诉。
3.报价人捏造事实、伪造材料，或者以非法手段获取证明材料进行质疑或者投诉的，将被列入黑名单管理；给他人造成损失的，依法承担赔偿责任。
4.异议受理单位
采购人：重庆长电渝电力工程有限公司
联系电话：15858189236
邮箱：CDYCQ2025@163.com
地址：重庆市两江新区聚贤岩广场 6 号力帆中心 1 号楼 27-5
5.投诉受理单位
重庆三峡水利电力（集团）股份有限公司
投诉电话：023-65437809
地址：重庆市北部新区金开大道升伟晶石公元 12 栋 1 楼

9. 需要补充的其他内容

9.1	首次采购有效供应商不足两家的处理原则	如经评审有效报价人仅一家，且其经济、技术等指标仍然具有市场竞争力，并满足采购文件要求的，评审小组可以继续评审并确定成交候选人。
9.2	重新采购的情形	有下列情形之一的，采购人将重新采购(首次采购适用): (1)响应截止时间止，报价人少于 2 个的； (2)经评审小组评审所有响应被否决的； (3)经评审有效供应商仅一家且其经济、技术等指标明显缺乏市场竞争力的。

第二章 评审办法

（最低报价法）

评审办法前附表

条款号		评审因素	评审标准
2.1.1	形式 评审 标准	报价人名称	与营业执照一致
		报价函签字盖章	有法定代表人（负责人）或者其委托代理人签字或加盖单位章
		报价文件格式	符合第五章“报价文件格式”的要求
		报价唯一	只能有一个有效报价
2.1.2	资格 评审 标准	法人证照	具备有效的合法登记证明文件
		资质要求	符合第一章“采购公告”第 3 项规定
		财务要求	无
		信誉要求	符合第一章“采购公告”第 3 项规定
		业绩要求	符合第一章“采购公告”第 3 项规定
		其他要求	符合第一章“采购公告”第 3 项规定
2.1.3	响应 性评 审 标准	报价	符合第一章“采购公告”最高限价相关规定
		内容	符合第四章“ 网络安全防护设计方案”相关规定
		交货批次与进度	符合第一章“采购公告”交货、安装调试及网安服务安排相关规定
		质量要求	符合第四章“ 网络安全防护设计方案”相关规定
		报价有效期	90 天
		报价担保	无
		报价表	符合第五章“报价文件格式 文件三 报价表”相关规定
		技术规范	符合第四章“ 网络安全防护设计方案”相关规定
条款号		量化因素	量化标准
2.2	详细评 审标准	技术偏差评审	评审小组核实存在技术偏差的报价是否等同或优于技术要求。不满足技术要求的报价将被否决。
		报价合理性评审	评审小组发现某项设备中报价人的报价明显

		低于其他报价，使得其报价可能低于其成本的，应当要求该报价人作出说明并提供相应的证明材料。报价人不能合理说明或者不能提供相应证明材料的，评审小组认定该报价人以低于成本报价竞价，否决报价人该项物资报价。
条款号	量化因素	量化标准
3.4.1	推荐成交候选人的顺序	评审小组按合格报价人的最终修正报价由低到高顺序推荐 <u>1-3</u> 名成交候选

1. 评审方法

本次评审采用最低报价法。评审小组对满足询价文件实质要求的报价文件（含报价文件澄清答复），按照不含税报价由低到高的顺序推荐成交候选人，但报价低于其成本的除外。经评审的报价相等时，报价低的优先；报价也相等的，由采购人自行确定。

2. 评审标准

2.1 初步评审标准

2.1.1 形式评审标准：见评审办法前附表。

2.1.2 资格评审标准：见评审办法前附表。

2.1.3 响应性评审标准：见评审办法前附表。

2.2 详细评审标准

详细评审标准：见评审办法前附表。

3. 评审程序

3.1 初步评审

3.1.1 评审小组可以要求报价人提交采购文件规定的有关证明和证件的原件，以便核验。评审小组依据本章第 2.1 款规定的标准对报价文件进行初步评审。有一项不符合评审标准的，评审小组应当否决其报价。

3.1.2 本次评审对于经过澄清后仍然存在下列情况之一的报价人的报价，将被视为未对询价文件进行实质上响应，不能进入下一阶段评审：

- (1) 串通报价或弄虚作假或有其他违法行为的；
- (2) 不按评审小组要求澄清、说明或补正的；
- (3) 资格条件不符合询价文件要求的；
- (4) 报价文件无法定代表人签字(或签字人无法定代表人有效授权委托书)和加盖单位公章的；
- (5) 报价有效期不满足询价文件要求的；
- (6) 项目实施方案不满足询价文件的要求的。

3.1.3 评审小组按以下原则对报价进行修正，修正的价格经报价人确认后具有约束力，报价人不接受修正价格的，评审小组应当否决其报价：

- (1) 报价文件中的大写金额与小写金额不一致的，以大写金额为准；
- (2) 总价金额与依据单价计算出的结果不一致的，以单价金额为准修正总价，但单价金额小数点有明显错误的除外。
- (3) 当分项合计报价与总报价不一致时，以各分项合计报价为准，修改总报价（此种情况下，总报价为修正总报价）；
- (4) 当税金与不含税总报价按税率取费金额不一致时，以不含税总报价按税率取费金额为准，修改总报价（此种情况下，总报价为修正总报价）
- (5) 缺漏项视为含在总报价中，缺漏项不进行算术错误修正。

3.2 详细评审

3.2.1 评审小组核实存在技术偏差的报价是否等同或优于技术要求。不满足技术要求的报价将被否决。

3.2.2 评审小组发现报价人的报价明显低于其他报价，或者在设有评审参考价时明显低于评审参考价，使得其报价可能低于其成本的，应当要求该报价人作出说明并提供相应的证明材料。报价人不能合理说明或者不能提供相应证明

材料的，评审小组认定该报价人以低于成本报价竞价，其报价作无效报价处理。

3.3 报价文件的澄清和补正

3.3.1 在评审过程中，评审小组可以要求报价人对所提交的报价文件中不明确的内容进行澄清或说明，或者对细微偏差进行补正。评审小组不接受报价人主动提出的澄清、说明或补正。

3.3.2 澄清、说明和补正不得改变报价文件的实质性内容。报价人的澄清、说明和补正属于报价文件的组成部分。

3.3.3 评审小组对报价人提交的澄清、说明或补正有疑问的，可以要求报价人进一步澄清、说明或补正，直至满足评审小组的要求。

3.4 评审结果

3.4.1 推荐成交候选人的顺序：见评审办法前附表。

3.4.2 评审小组完成评审后，应当向采购人提交书面评审报告。

3.4.3 成交候选人在信用中国网站（<http://www.creditchina.gov.cn/>）被查询存在与本项目相关的严重失信行为，评审小组认为可能影响其履约能力的，有权取消其成交候选人资格。

中共重庆长电渝电力工程有限公司
会议签到表

会议名称	学习贯彻党的二十届四中全会精神补学会		
会议地点	27楼大会议室		
会议时间	2026年4月2日		
主持人	赵春霞		
签 名 栏			
序号	部门/单位	姓名	备注
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

21			
22			
23			
24			
25			
26			
27			
28			
29			
30			
31			
32			
33			
34			
35			

第三章 合同条款及格式

物资采购合同

合同名称：水风光多能互补联合实验室鱼背山科研成果验证基地建设 EPC 工程总承包项目网络安全防护设备采购

合同编号：_____

甲方（买方）：

乙方（卖方）：_____

签订地点：

买方：_____

卖方：_____

_____（以下简称“买方”）拟向_____（以下简称“卖方”）采购网络安全防护设备（以下简称“合同物资”），且卖方同意向买方出售上述合同物资。根据《中华人民共和国民法典》，买卖双方经友好协商，同意按下述条款签署本合同。

1.合同物资采购期限、交货日期、交货地点及其他要求

1.1 合同物资名称、规格、单位、数量、价格等详见附件 1：《设备清单》。

1.2 合同物资交货及安装调试及网安服务日期：合同签订后卖方一次性将全部合同物资运送至合同指定交货地点。物资全部到货后，卖方须按买方通知要求，于 45 日内完成设备安装调试及网安服务工作。卖方发货前 2 日须与买方沟通确认，不得擅自发货。

1.3 交货地点：由卖方负责将合同物资送达买方指定位置，具体地址以买方通知为准，且卖方应在装运后 24 小时之内以传真或函件形式将合同号、合同物资名称、数量、运输工具及启运日期通知买方。

1.4 网络安全服务内容及要求：卖方需无偿提供漏洞扫描、协助安全加固、等保合规培训、现场首次整改指导等内容，须在设备供货、安装调试全部完成并整体竣工验收前实施完毕（1 年免费远程技术咨询服务在质保期内，不在本次验收范围），纳入项目整体竣工验收范围，要求详见附件 2 网络安全防护设计方案。

2.合同价款

2.1 本合同含税总价为人民币（大写）：_____（¥_____元），不含税总价为人民币（大写）：_____（¥_____元），增值税税率____%。合同约定的税率与国家税法规定及税务机关认定的税率不一致时，以国家税法规定及税务机关认定的税率为准，调整时以不含税价为基准，执行国家法规规定及税务机关规定的税率。

2.2 本合同具体价格构成详见《设备清单》。本合同价格已包括了合同中规定的卖方应承担的全部义务以及为实施和完成本合同项下全部义务和责任所必需的一切费用，

买方除此之外无需再向卖方支付或承担其他任何费用，卖方不得要求除本合同明确约定应由买方承担的其他任何费用，包括但不限于与本合同相关的合同物资成本、损耗、运输费、保险费、包装费、装载费、验收检验检测费、现场指导费、设备安装调试、培训服务等为完成本合同约定的所有内容的费用。

2.3 合同价格采用以下 2.3.1 形式：

2.3.1 固定单价合同。

(1) 详见附件 1：《设备清单》；

(2) 其他： /。

2.3.2 固定总价合同。

2.3.3 其他方式： /。

2.4 合同价款变更。

2.4.1 合同价格采用固定单价形式时，合同设备数量变更导致实际合同设备数量与《设备清单》发生变化，最终结算按实际采购合同物资数量对《设备清单》据实结算，单价不予以调整。

2.4.2 合同价格采用固定单价形式时，《设备清单》中无适用、但有类似于变更合同设备的，可在合理范围内参照类似合同设备的综合单价；《设备清单》中无适用或类似子目综合单价的，应结合现行市场行情，由合同双方当事人协商后确定综合单价。

2.4.3 合同价格采用固定单价形式时，合同执行期内因物价波动、法规更改等情形引起的价格变动，单价不予以调整。

2.4.4 合同价格采用固定总价形式时，合同执行期内因物价波动、法规更改等情形引起的价格变动，总价不予以调整。

3.质量及技术要求

3.1 卖方保证全面按合同《设备清单》规定的品牌、参数、技术标准和数量提供全新的、完整的和符合质量及技术要求的合同物资；

3.2 卖方应提供合同物资的出厂合格证、产品型式检查报告、计算书等技术资料（进口合同物资需提供原产地证明、海关商检报关单等）；若卖方无法及时提供相关资料，买方有权迟延付款；

3.3 卖方提供的合同物资应符合国家标准、行业标准、企业标准和双方约定的合同物资技术要求，并符合国家环境保护和职业健康安全等相关法律法规的要求（进口合同

物资需符合国际标准)。使用的标准应是已颁布的最新版本,并按较高标准的条款执行。凡属国家 3C 强制认证范围的产品,必须贴有 3C 认证标签;

3.4 卖方保证所供合同物资符合国家环境保护和职业健康安全等相关法律法规的要求;

3.5 卖方开展设备安装调试工作须严格遵照合同技术标准及要求实施,全部作业完成后须经买方验收合格方可视为安装调试完成;

3.6 其他要求: / 。

4.包装及运输

4.1 卖方用于合同设备的包装材料,应符合国家和地方相关环保标准。用于合同物资的包装材料有特殊要求的,由双方另行约定。合同物资包装应适应多次搬运和远距离运输,以保证合同物资安全无损地抵达买方指定的位置。如因包装或运输原因造成合同物资受损、瑕疵、贬值,买方有权拒收合同物资,卖方应当无条件退换,并承担相关责任和损失。

4.2 合同设备的包装、装载、运输及保险费用由卖方承担。卖方应根据合同物资的不同形状和特点,采用相应防潮、防锈、防震、防腐等必要保护性措施的坚固包装。

4.3 合同设备的包装应遵守所有可适用的特殊要求,包括但不限于危险品的包装要求。

4.4 小件合同设备及松散零星的部件应采用适当的包装方式,装入小的完好的包装袋内,并整车发运。

4.5 卖方交付的合同设备技术资料应装订成册并使用适合于长途运输、多次搬运和防潮的包装。每一包资料内应附有技术资料的详细清单一式二份,标明技术资料的序号、文件项号、名称和页数的明细表。

4.6 凡重量达到 2 吨的合同设备或特殊形状的合同物资,应在包装箱的侧面以运输常用的标记和图案标明重量及起吊位置,以便于装卸搬运。按照合同物资的特点,装卸和运输上的不同要求,包装箱上应明显地印刷“禁止溜放”、“勿倒置”、“防雨”等字样,标有适当的习惯用符号和直观标记。

4.7 卖方应对承运人履行所有应尽的说明义务,包括但不限于对危险物品的名称、危险性质、必要时应当采取的预防措施等进行的说明。因卖方未尽该等义务与承运人发生的任何争议或因此产生的任何后果,均由卖方承担,与买方无关。买方因此受有

损失的，卖方负责赔偿买方。

4.8 其他要求： / 。

5. 交货方式

5.1 卖方的交货清单和本合同第 3 条“质量及技术要求”约定的产品质量证明文件等所有相关资料应在交货时一并向买方提供，且与实物相符，否则买方有权拒收并按卖方迟延交货处理，并视为卖方违约。

5.2 卖方在交货时应提供合同物资及主要部件出厂合格证、产品型式检查报告、计算书、检测报告等资料。

5.3 合同物资的所有权及风险自合同物资送达指定位置并交付给买方时起转移至买方，但因卖方交付合同物资经验收不符合合同约定，买方向卖方发出拒收合同物资或解除本合同的通知之时起，合同物资毁损灭失的风险由卖方承担。

6. 验收

6.1 全部符合合同要求的合同物资到达合同约定的交货地点，卖方提交书面验收申请后，买方在 3 个工作日内完成验收。

6.2 按合同质量技术要求核验物资性能、安装调试成果，检验合格后签署验收报告，并组织进行网络安全服务，当服务内容、交付物、资质资料全部达标后即为验收通过。

6.3 除另有约定外，按合同约定的质量及技术要求对合同物资的各项性能指标进行检验合格后，由买方签署验收合格报告，视为验收合格。

6.4 对验收不能满足合同要求的合同物资，买方有权选择以下一种或几种补救措施，由此发生的费用由卖方承担：

6.4.1 修理。卖方对不符合合同约定的合同物资进行修理（含返厂维修），以使其符合合同要求，费用由卖方承担。除非买方同意，修理工作应在 30 日以内完成。逾期未完成的，按照本合同第 10 条“违约责任”向买方支付违约金。卖方修理的合同物资仍不符合合同要求的，买方有权要求更换、向第三方采购可替代货物或解除合同。

6.4.2 更换。卖方以符合合同要求的货物替换不符合合同要求的合同物资，费用由卖方承担。除非买方同意，更换应在 30 日以内完成。逾期未完成的，按照本合同第 10 条“违约责任”向买方支付违约金。卖方更换的货物仍不符合合同要求的，买方有权要求退货、向第三方采购可替代货物或解除合同。

6.4.3 退款退货。买方将有缺陷的合同物资退还卖方，卖方负责将被退还的合同物

资运出安装现场，且卖方应退还已收取的该合同物资的全额货款并承担该合同物资的安装、拆卸、运输、保险及购买替代品的差价等费用。

6.4.4 降减合同物资价格。在买卖双方同意的前提下，对有缺陷的合同物资作降减价格处理，卖方应将将有缺陷的合同物资原合同价与降减后价格之间的差额退回买方。

6.4.5 向第三方采购。买方有权依其认为适当的条件和方法向第三方采购可替代的货物，由此发生的差价、增加的费用和损失等由卖方承担。

6.5 买方选择以上任何补救措施均不减轻或免除卖方依据合同所应承担的违约责任并赔偿因此给买方造成的全部损失。

6.6 其他约定： / 。

7.权利和义务

7.1 买方权利和义务

7.1.1 合同物资技术指标不满足本合同约定要求的，买方有权退货、更换或向第三方采购可替代物资，由此造成买方的损失以及产生的费用均由卖方承担。买方选择更换的，卖方应及时进行更换并承担全部费用，且更换周期应满足工期要求，否则卖方应承担违约责任；

7.1.2 买方有权要求卖方提供原材料材质和性能检测报告、外购零部件试验报告及合格证、关键工艺说明、货物检验和试验报告等资料，其中对关键的原材料和零部件要求有供货批次、日期记录和质量控制标准。

7.1.3 买方有权对合同物资（包括原材料、元器件、关键工艺、成品等）在交货前进行检验，或委托第三方检验机构实施抽检。买方自行或委托第三方检验机构实施抽检的，如抽检的合同物资符合合同要求，所有检测等相关费用由买方承担；如抽检的合同物资不符合合同要求，买方有权按照合同约定或国家相关规定，扩大抽检范围，并根据检测结果及合同相关约定，要求卖方采取重新生产、修理、更换、向第三方采购可替代物资等补救措施或单方解除合同，同时所有检测、运输等相关费用由卖方承担；

7.1.4 根据工作需要，协助卖方完成相关工作；

7.1.5 负责合同物资及其备品备件、专用工具等附属物的验收；

7.1.6 按照合同约定向卖方支付合同价款。

7.1.7 买方负责免费提供设备安装所需现场场地、机房环境、电源、网络基础条件，

协调现场相人员配合卖方开展安装、布线、调试、验收工作；及时确认安装调试方案，因买方配合延误造成工期滞后的，工期相应顺延。

7.1.8 其他： / 。

7.2 卖方权利和义务

7.2.1 卖方有权按合同约定向买方收取合同价款；

7.2.2 卖方承诺按合同约定向买方提供符合要求的合同物资和服务；

7.2.3 未经买方同意，卖方不得将本合同项下的债权（合同价款及其他权利）转让给任何第三方、向任何第三方提供担保或者办理保理事项；

7.2.4 卖方保证其依照本合同向买方交付的合同物资依法拥有完整所有权，合同物资上不存在任何抵押、质押、留置等担保物权、任何第三方知识产权，不存在任何性质的附属或者限制性权益，也不存在被任何政府机关或者司法机关查封、扣押、冻结的情形。卖方对物资享有合法完整的所有权、知识产权及其他相应的权利；

7.2.5 卖方保证买方不会因为合同物资侵犯任何知识产权而被提起索赔、指控或请求，否则，卖方应当就买方因此遭受的损失（包括但不限于直接损失、间接损失、律师费、诉讼费或仲裁费等）承担全部赔偿责任；

7.2.6 卖方保证其供应的合同物资是全新的（未使用过的）、安全的、技术水平先进的、成熟的、质量优良的，未侵犯任何第三方的知识产权，合同物资的选型符合安全可靠、经济运行和易于维护的要求。合同物资的技术规范、技术经济指标和性能应符合本合同约定的要求；

7.2.7 执行合同过程中发现合同约定的合同设备材料、技术资料、专用工具、备品备件和技术服务有任何漏项和短缺，而该遗漏或短缺部分确实是卖方供货范围中应该有的，并且是满足合同约定的性能保证值所必须的，卖方均应负责将遗漏或短缺的部分补上，发生的费用由卖方承担；

7.2.8 卖方应委派数量足够、经验丰富、资质合格且具备相关专业技术工作经验的技术人员，按照买方要求赴现场提供技术服务、技术培训及技术指导；

7.2.9 由于卖方未提出明确要求或者买方按照卖方要求进行仓储保管，导致合同物资在保管期间发生损坏的，卖方应承担由于修理和/或更换损坏的合同物资而发生的一切费用；

7.2.10 卖方负责办理合同物资从出厂至指定的交货地点运输途中的保险，被保险

人为卖方，保险范围应包括卖方负责运输的全部合同物资，险种为合同物资价值 120% 的“一切险”，保险费由卖方承担。卖方应在发货 5 日前向买方出具相关投保证明；

7.2.11 卖方技术人员在现场提供技术服务时应接受现场的监督管理；在施工现场未经许可，不得拆卸、涂抹、损坏任何合同物资；卖方如需对合同物资进行调试，应在现场监理代表的监督下进行操作，必要时须经过现场监理代表或业主项目部负责人的同意。若卖方技术人员违反现场安全规定，引起的一切后果，由卖方承担；

7.2.12 在合同履行过程中，对由于卖方原因需要进行的检查、试验、再试验、修理或更换，卖方应承担进行上述工作所需的费用，买方协助做好安排以便进行上述工作；

7.2.13 卖方提供的合同物资如有缺陷，或由于技术资料有错误、卖方技术人员指导错误，造成合同物资报废或工程返工，卖方应立即无偿进行更换或赔偿买方因此遭受的损失。需更换合同物资的，卖方应承担由此产生的到安装现场换货的一切费用，包括但不限于新货物的费用、将新货物运至安装现场的费用及处理被更换货物的费用等。卖方更换或修理合同物资的期限按买方要求执行，如逾期未完成更换或修理工作的，按延迟交货处理；

7.2.14 合同物资验收投运后 1 年内出现喷漆脱落、锈蚀等任何影响合同物资外观的损坏，卖方应免费处理；

7.2.15 合同物资存在家族性缺陷的，卖方应主动召回；

7.2.16 卖方须严格遵照国家规范、行业标准、设计方案及买方要求组织施工安装调试，做好现场安全文明施工，承担施工期间人身、设备、消防安全全部责任，发生安全事故由卖方承担全部损失及法律责任。

7.2.17 其他： / 。

8.质量保证期

8.1 合同设备质量保证期自全部设备完成安装调试验收合格网安服务完成之日起计算 365 天。若法律法规、国家及行业标准规定质保期长于本合同约定的，按较长期限执行。

8.2 质保期内，因卖方原因造成物资故障、损坏、停运的，维修、更换完成并经甲方重新验收合格后，对应故障部件及整台设备质保期自重新验收合格之日重新起算。仅部件缺陷不影响整体运行的，维修更换后部件质保期重新计算。

8.3 质保期内卖方提供免费维修、更换服务。卖方接到甲方售后通知后 24 小时内到场，48 小时内恢复设备正常运行并满足合同技术要求。卖方逾期到场、逾期未修复的，甲方有权委托第三方维修，费用由卖方承担，可直接从质量保证金/质量保函中扣除；不足部分卖方另行赔偿。质保金支付抵扣不免除卖方质保责任。

8.4 质量保证期的届满不能视为卖方对合同设备中存在的可能引起合同设备损坏的潜在性缺陷所应负责任的解除。质量保证期结束后 1 年内，合同物资出现潜在性缺陷时，买方有权要求卖方对有缺陷的合同设备和同一批次的合同设备免费予以及时修理或更换。

8.5 其他约定： / 。

9.付款方式

9.1 本合同结算货币为人民币。

9.2 款项均以银行转账形式支付。

9.3 合同价款按如下节点支付：（1）全部设备到货并经买方验收合格，乙方提交对应等额增值税专用发票及验收资料，甲方审核无误后 30 日内，支付合同总价 70%进度款。（2）设备安装调试全部完成且验收合格，网安服务按进展要求完成，乙方补齐剩余合规发票及全套竣工资料，甲方审核无误后 30 日内，付款至合同总价 97%。（3）剩余合同总价 3%作为质量保证金。质保期为 1 年，缺陷责任期满，设备无质量隐患、运行状态正常、1 年免费远程技术咨询服务按买方要求开展到期，乙方提交结清申请及缺陷责任期终止证明，甲方核验无误后 30 日内无息返还质保金本金。

9.4 每次付款前，乙方须按国家规定开具合规等额增值税专用发票，未按要求提供发票的，甲方不予对应款项支付。

9.5 卖方收款账户信息以合同签署页为准，因自身账户信息问题引发的损失，由卖方自行承担。

9.6 卖方变更收款账户须提前出具书面通知，未及时告知产生的损失由卖方自负。

10.违约责任

10.1 除法定原因外，买卖双方任何一方不履行或不能履行合同义务时，应当向对方支付合同总价 20% 的违约金，另一方有权解除合同，任何一方造成对方损失超过违约金的，超出部分由违约方继续承担赔偿责任。

10.2 卖方未能在合同约定交货日期内履行交货义务即为卖方迟延交货，自应交货

期限之次日起，每迟延一天则按合同总价的 1% 向买方偿付违约金，并赔偿买方遭受的损失；若卖方迟延交货超过 15 天以上的，买方有权单方解除合同，卖方应向买方支付合同总价 20% 的违约金并赔偿损失。

10.3 卖方交付的合同物资不符合数量、质量要求，买方可选择要求卖方在 10 日内对不合格产品予以更换，更换期间按本合同第 10 条“违约责任”第 10.2 款“卖方延迟交货”处理，如更换后仍不能满足要求的，买方有权单方解除合同，卖方应向买方支付合同总价 20% 的违约金并赔偿损失。

10.4 若买方延迟付款，自应付款期限之次日起，每迟延一个工作日则按延迟付款金额的 1% 向卖方支付违约金。

10.5 卖方根据本合同第 10 条“违约责任”需支付各项违约金累计达到合同价格的 30% 时，买方有权退货或解除合同。卖方应退还买方已支付的全部合同价款，并自费将所交付的合同物资（如有）运离现场。买方因退货所产生的费用，包括安装费用、拆卸（除）费用、另行采购合同物资所发生的额外费用等及其他相关损失由卖方承担。

10.6 未经买方同意，卖方不得擅自变更合同物资原材料供应商，否则买方有权拒收所涉及的合同物资，并有权要求卖方支付人民币 30000 元违约金。卖方支付的违约金低于给买方造成的损失，应就差额部分向买方进行赔偿。

10.7 因卖方违约导致买方应向第三方赔偿损失（包括但不限于窝工损失等），该损失由卖方承担。买方先行承担的，有权向卖方追偿。

10.8 卖方应确保增值税发票真实、规范、合法，如卖方虚开或提供不合格的增值税发票，造成买方经济损失的，卖方承担全部赔偿责任，并重新向买方开具符合规定的增值税发票。

10.9 若卖方出现本合同第 10 条“违约责任”任一违约情形，买方均有权从待付价款中直接扣除卖方应当向买方支付的违约金或损害赔偿款。

10.10 未经买方同意，卖方不得将本合同下的义务对外分包。未经买方同意卖方擅自分包的，卖方应承担合同价格 30% 的违约金。买方有权拒收分包部分合同物资，并按照本合同第 10 条“违约责任”第 10.2 款“卖方延迟交货”追究卖方延迟交货的违约责任。

10.11 买方违反合同约定延迟支付合同价款的，应就逾期部分向卖方支付按照中国人民银行规定的同期贷款基准利率计算的逾期付款违约金。

10.12 卖方未按本合同约定 45 日历日内完成全部安装调试并通过验收的应向买方解释原因，若买方不认可卖方的原因，每逾期一日按合同总价 1%向买方支付违约金。

10.13 因卖方安装施工不规范、配置错误、调试不达标造成一次验收不合格的，卖方须在 7 日内无偿整改完毕；二次验收仍不合格的，买方有权扣除合同总价 1%作为违约金，同时卖方仍需无条件整改直至合格。

11.不可抗力

11.1 “不可抗力”指不可预见、不能避免并不能克服的、影响合同义务履行的所有事件，包括但不限于地震、台风、海啸、暴风雪、泥石流、山体滑坡、战争、火山、龙卷风、核辐射、瘟疫、骚乱、武装冲突、罢工、政府行为等。

11.2 如不可抗力的发生致使合同一方履行义务受到影响，该方应自不可抗力发生之日起 3 天 内以书面形式通知另一方，同时积极采取合理措施，减少因不可抗力给另一方带来的损失，承担因未采取合理措施所导致的扩大损失。该方在不可抗力发生之日（如遇通讯中断，则自通讯恢复之日）起 15 日内将不可抗力发生地相应权威机构出具的证明文件提供给另一方确认。

11.3 对于本合同中未受不可抗力直接影响的其它义务，义务方必须继续履行。如果不可抗力阻碍一方履行义务持续超过 120 日，双方应协商决定继续履行、变更或终止本合同。如双方不能达成一致意见，任何一方有权通知另一方解除合同，本合同另有规定除外。

11.4 双方当事人应在不可抗力事件结束或其影响消除后立即继续履行其合同义务，合同期限也应相应顺延。如果不可抗力事件的影响可能造成卖方无法完成合同履行，双方可协商解除本合同。由于合同解除所引起的后续问题由双方友好协商解决。

12 争议解决

12.1 因本合同发生争议，双方应当协商解决。不愿协商或者协商不成的，采用以下所列第 12.1.2 种方式解决：

12.1.1 向重庆仲裁委员会申请仲裁。

12.1.2 向合同签订地的人民法院提起诉讼。

12.2 在争议解决期间，合同中未涉及争议部分的条款仍须履行。

13.其它

13.1 本合同自双方法定代表人或授权代表签署并加盖双方公章或合同专用章之日

起生效。

13.2 卖方完成所有合同约定的工作内容且经买方验收合格，买方付清所有款项后，合同双方均未遗留按合同约定应履行的义务时，合同自然终止。

13.3 在合同履行过程中，其他未尽事宜或需对合同进行变更，双方应签订书面协议，并经双方法定代表人（单位负责人）或其授权代表签字并加盖公章或合同专用章后生效。补充协议与本合同附件是本合同不可分割的组成部分，具有同等法律效力。

13.4 本合同一式陆份，其中正本贰份，双方各执一份，副本肆份，买方执叁份，卖方执壹份。均具有同等法律效力。

合同附件

附件 1：设备清单；

附件 2：网络安全防护设计方案；

附件 3：设备安装安全环保协议；

附件 4：网络安全协议；

附件 5：廉洁协议；

附件 6：保密协议；

附件 7：合规承诺函。

（以下无正文）

(合同签署页)

买方（盖章）：	卖方（盖章）：
法定代表人 或其授权代理人（签字）：	法定代表人 或其授权代理人（签字）：
签署日期： 年 月 日	签署日期： 年 月 日
地址：	地址：
邮政编码：	邮政编码：
联系人：	联系人：
联系电话：	联系电话：
传真：	传真：
开户银行：	开户银行：
账号：	账号：
开户行联行号：	开户行联行号：
统一社会信用代码：	统一社会信用代码：

附件1

设备清单

序号	设备名称	推荐品牌	参数(参数中的所有要求需全部满足)	数量	单位	报价品牌	报价参数	含税单价 (元)	含税总价 (元)
1	防火墙	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
2	堡垒机	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
3	数据库审计	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
4	终端安全及防病毒系统	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	套				
5	EDR 管理中心服务 器	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
6	服务器操作系统	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	套				
7	APT 攻击预警平台	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
8	入侵检测	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				

9	恶意代码防护	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	1	台					
10	纵向加密机	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	2	台					
11	交换机	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	2	台					
12	路由器	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	1	台					
13	反向隔离装置	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	1	台					
14	网监 II 装置	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	1	台					
15	探针	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	6	套					
16	通信 330 以太网板	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	2	块					
17	对时装置	/	详见“第四章 网络安 全防护设计方案, 5.1 设备清单”	1	套					
含税总价										

注：增值税专票税率为_____。

(1) 交付前的一切风险由卖方承担；

(2) 卖方的综合单价包含但不限于与本合同相关的合同物资成本、税金、损耗、运输费、保险费、包装费、装卸费、仓储费、验收检验检测费、操作培训费以及卖方委派人员的差旅费、食宿费等为完成本合同约定的所有内容的费用；

(3) 所有设备、材料必须有出厂合格证及质量证明书；

(4) 设备及材料非买方原因损坏的，由卖方免费返厂检修或及时更换，检修费用（包括但不限于邮寄费等）由卖方承担。

(5) 其中 1-17 项包含安防设备安装调试（包括但不限于提供所需的人力、设备、物料完成二次安防设备的安装调试工作。）及网安服务（包括但不限于设计方案中要求的漏洞扫描、整改指导服务、协助加固、合规培训服务、应急支持服务（要求详见详见“网络安全防护设计方案， 5.2 服务清单”）。卖方在提供整改指导服务时，为确保准确识别与等级保护基线配置要求的差距，应采用专业的网络安全等级保护检查工具箱作为服务工具，且服务工具需具备中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）兼容性资质证书，提供证书复印件并加盖制造商公章。卖方在提供漏洞扫描服务时，应采用专业的 web 应用漏洞扫描服务工具与数据库漏洞扫描服务工具，且服务工具需具备中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）兼容性资质证书，提供证书复印件并加盖制造商公章。）安防设备安装调试及网安服务的价格包括在 1-17 项价格当中，不在单独计价。

附件2

网络安全防护设计方案

详见“第四章 网络安全防护设计方案”

附件 3:

设备安装安全环保协议

发包单位: _____ 以下简称“甲方”。

承包单位: _____ 以下简称“乙方”。

为加强工程项目安全文明施工和环境保护管理,依据国家和当地有关法律、法规、规章等有关规定和要求,甲乙双方在签订工程项目合同的同时,经协商一致,签订本协议。

一、工程概况

1. 项目名称: _____。
2. 项目地点与范围: _____。
3. 承包主要内容: _____。
4. 工程项目期限: 自 _____ 年 _____ 月 _____ 日起 _____ 年 _____ 月 _____ 日止。

二、协议内容

(一) 安全文明施工与环境保护目标

1. 不发生重伤及以上人身伤亡事故,不发生电力安全事故、电力安全事件及设备障碍,不发生火灾事故以及在甲方现场发生同等及以上责任交通事故;
2. 不发生突发环境事件,不发生违法排污责任事件或其他环境违法行为;
3. 符合安全生产、环境保护法律法规和标准规范的规定,达到甲方提出的现场安全环保文明施工要求。

(二) 甲方的安全文明和环境保护权利和义务

1. 甲方是项目的安全生产与环境保护的监管主体,负责工程项目安全生产和环境保护工作的统一协调、管理。
2. 对乙方的管理人员及作业人员的安全资格进行核查,对核查材料存档保管。乙方资质、资格不符合规定或提供虚假核查材料的,甲方有权要求乙方更换人员或终止合同,且不承担赔偿或补偿责任。
3. 组织项目施工前的安全技术交底,收集提供施工现场临近带电设备、地下管线等相关资料,并提出保护措施要求。向乙方的负责人、工程技术人员及相关管理人员环境保护技术交底,提出包括噪声、污水、扬尘与尾气排放、废弃物和垃圾分类管理等方面的环保要求。
4. 根据要求对乙方组织相关安全教育培训,督促乙方对全体施工人员进行入场安

全教育和安全知识考试，审查备案乙方安全教育记录和考试记录。

5. 对乙方施工机械设备、工器具和安全防护设施进行监督。

6. 甲方在施工期间指派_____负责本项目的安全环保文明生产管理与监督。

7. 组织现场安全环保监督检查，纠正违章行为，提出整改意见，进行考核。对查出施工中安全环保隐患整改不力的，有权要求乙方停工整顿或解除合同，相关责任由乙方承担。

（三）乙方的安全文明施工和环境保护权利和义务

1. 乙方是项目的安全环保施工责任主体，负责施工现场的安全生产管理、环境保护管理；服从甲方对现场安全文明施工和环境保护的监督管理。乙方项目负责人为_____，乙方更换项目负责人或安全环保负责人需报甲方审批。

2. 乙方在甲方场地或甲方指定的场地提供服务过程中，严格执行国家和地方政府的相关法律法规要求，鉴于甲方已建立了安全生产和环境保护管理制度和规定，乙方在甲方场地提供服务期间，应遵守甲方的相关规定；若乙方是在甲方指定之第三方场地提供服务的，应同时遵守场地方的相关规定(如有)。

3. 工程开工前，乙方应开展现场勘查，编制施工组织设计、施工方案和安全环保技术措施并报甲方或甲方指定的第三方单位同意，安全技术措施中应明确验收要求。对于复杂自然条件、复杂结构、技术难度大及危险性较大的分部分项工程（以下简称“危大工程”）施工前编制专项施工方案，对超过一定规模的危大工程专项施工方案组织符合专业要求且持有专家证明的专家论证。危大工程严格落实《危险性较大的分部分项工程安全监督管理规定》（住房和城乡建设部令第37号）等相关安全管理规定。

4. 乙方应在作业现场设置防触电、防坠落、防火、防爆炸、防中毒、防扬撒、防流失、防渗漏等安全环保防护设施；防止或者减少粉尘、废气、废水、固体废物、噪声、振动和施工照明对人和环境的危害和污染，做到合规排放；防止有毒有害物品、危险品的泄漏、遗洒、挥发、扩散和随意丢弃；施工废物及时清运。

5. 指定工作负责人办理生产区域工作票许可手续，指定专职安全监护人并保证其在作业现场实行连续监护，严禁在无专人监护的情况下从事爆破、吊装、动火、临时用电、有限空间、高处作业、临近带电体作业等危险作业。

6. 乙方聘请的在甲方场地或甲方指定的场地向甲方提供服务的员工必须符合国家劳动法规要求，有合法的用工手续并签订用工合同，配备合格、适用的工作服、安全帽、安全带、口罩、护目镜、手套等个人防护装备，并督促作业人员正确使用；着装、标识统一（须与甲方工作人员的着装、标识有所区别）；乙方人员进入甲方场地

或其它特定场地（包括甲方指定的第三方场地），应同时遵守该场地的劳防用品佩戴规定（如有）。

7. 对甲方提供的设施设备、工具等是否能够满足预期的任务进行仔细检查和评估，合格方可使用。合理使用甲方提供的设施设备、工具等，对错误使用或不当使用甲方提供的设施设备、工具所造成的损失损害由乙方自行承担。

8. 对全体管理人员和施工人员进行入场安全技术培训、教育，安全知识考试和每日危险源、环境因素的辨识活动，并保存相关记录备查，考试不合格者不得入场工作。

9. 组织施工现场安全环保隐患排查治理；接受甲方和/或甲方指定第三方的安全、环保、防火、治安等的监督检查和管理，认真落实提出的隐患（不符合）整改意见，在规定期限内完成整改并报甲方和监理单位复验。

10. 发生人员伤亡、职业危害、设备财产损失、火灾事故、交通事故、突发环境事件的，现场人员应立即报告本单位负责人、监理负责人和甲方负责人；按国务院及地方政府有关事故报告规定及时报告政府监管部门；同时启动现场应急预案（或处置措施），抢救伤员，控制事故，保护现场，接受事故调查处理。

11. 不得擅自变更或改变甲方或甲方指定第三方所提供厂房、办公场地、电力线路以及设施设备的建筑结构和用途、使用性质等。若需搭建临时设施时必须事先经过甲方和甲方指定第三方（当乙方在甲方指定的第三方场地提供现场服务时）的书面同意。

12. 未经甲方（或甲方指定之第三方）许可，不得擅自将电气设备接入甲方（或甲方指定之第三方）的电气线路。如有违反，乙方承担由此产生的一切损失，并赔偿甲方和/或甲方指定之第三方因该违规行为所遭受的损失。

13. 只有在得到甲方（及甲方指定之第三方）同意后才能携带危险化学品进入甲方场地（或甲方之指定第三方场地）。

14. 乙方在施工或服务过程中的噪声排放应符合国家及地方法律法规、标准及甲方相关管理要求。

15. 建设项目未正式移交甲方前，乙方应负责施工过程中产生的建筑垃圾和其他废弃物的处置，相关废弃物的收集、贮存、运输和处置必须符合国家、地方法律法规及甲方环境管理要求。

16. 有权对甲方或甲方指定的第三方单位在施工安全环保管理工作中存在的问题提出改进意见，有权拒绝违章指挥和强令冒险作业。

（四）安全文明生产及环境保护考核标准

1. 由于乙方责任造成甲方或第三方的人身伤害、设备损坏等财产损失，由乙方承担一切经济损失和违约责任。

2. 由于乙方原因发生安全环保事故（事件）的，由乙方支付甲方违约金，并赔偿甲方因此遭受的损失，甲方有权在合同结算时扣减。违约金支付标准如下：

（1）发生人身轻伤事件，每人次支付不低于 1 万元违约金；发生人身重伤事故，每人次支付不低于 5 万元违约金；发生人身死亡事故，每人次支付不低于 10 万元违约金。

（2）发生一般级别的设备事故、电力安全事故、火灾事故、突发环境事件的，每次支付不低于 10 万元违约金；发生较大及以上级别的，每次支付不低于 20 万元违约金。

（3）发生安全环保事故（事件）后违约金支付金额超过合同金额的，以合同金额为限支付；乙方存在瞒报、谎报、迟报、漏报等情形的，加重处罚；重复发生上述事故（事件）的，甲方保留加倍处罚的权利。

（4）其他安全文明生产及环境保护考核标准和要求，按本协议附件：《安全环保管理补充规定》执行。

（五）需要补充协议内容：_____。

甲方单位（公章）：

乙方单位（公章）：

法定代表人或其

法定代表人或其

委托代理人（签字）：_____

委托代理人（签字）：_____

日期： 年 月 日

日期： 年 月 日

附件 4:

网络安全保密协议

甲方: _____

乙方: _____

因乙方为甲方提供产品与服务,已经(或将要)知悉甲方信息系统相关信息及甲方保密信息,为了明确乙方的网络安全保密义务,保证承建或提供服务的信息系统及信息设备的安全,防止甲方信息系统及其他保密信息被泄露,根据《中华人民共和国网络安全法》《中华人民共和国民法典》《中华人民共和国反不正当竞争法》《中华人民共和国计算机信息系统安全保护条例》和《计算机信息网络国际联网安全保护管理办法》等法律法规,甲乙双方本着平等、自愿、公平和诚实信用的原则,签订本网络安全保密协议,构成主合同的组成部分。

第一条 网络安全秘密

1. 本协议所称网络安全秘密包括但不限于信息系统平台架构、网络拓扑结构、硬件配置信息、安全加固措施、安防设备配置信息、安全防护策略、信息系统架构、程序源代码、通信协议、账号与密码信息、信息系统中的数据等,甲方提供用于完成主合同约定事项的各项资料、文件及电子数据、磁或纸介质文件、图片、影像资料,以及其他被甲方列为网络安全秘密的信息。乙方应对甲方网络安全秘密承担保密义务。

2. 甲方依照法律规定和在有关协议中的约定(如技术合同),需要乙方承担的与网络安全相关的保密义务,也属本协议的范畴。

本协议之签订可认为甲方已对公司的网络安全秘密采取了合理的保密措施。

第二条 乙方的义务

1. 乙方应遵守《中华人民共和国网络安全法》《电力监控系统安全防护规定》《信息安全等级保护管理办法》等法律法规对网络安全与信息保密的要求,以及甲方网络安全和保密的相关制度,并在设备及系统的全生命周期内对其负责。

2. 乙方应妥善保管甲方提供的用于完成交办任务的网络安全秘密(包括但不限于资料、文件及电子数据、磁或纸介质文件、图片、影像资料等),防止丢失和被盗。并承诺不会擅自复制(复印)用于完成交办任务的各项资料、文件及电子数据、磁或纸介质文件、图片、影像资料等;确因工作需求的,必须请示甲方同意。乙方不得将

用于完成交办任务的电子数据、资料、文件及磁或介质文件、图片、影像资料存储或拷贝在可接入互联网的设备、终端及移动存储介质上，同时须使用物理隔离的单机或光盘保存。

3. 甲方网络安全秘密只限于乙方的指定参与人员或单位知悉，不得擅自扩大知悉范围。乙方应与其知悉甲方网络安全秘密的乙方人员参照此协议签订相关网络安全保密协议，并向甲方备案，以确保知悉甲方网络安全秘密的乙方人员（包括该人员在退出项目或离职之后）遵守本协议约定的保密义务。

4. 乙方未经授权，不得擅自披露、使用甲方网络安全秘密；不得向不承担保密义务的任何第三人披露甲方的网络安全秘密；不得复制或公开包含甲方网络安全秘密的文件或文件副本；对工作过程中所形成的记录、数据、结果等，不得以任何形式携出甲方单位，或泄露给他人。

5. 乙方如果发现甲方网络安全秘密被泄露，或者因自己过失泄露了甲方网络安全秘密，应当采取有效措施防止泄密进一步扩大，并及时向甲方报告。在甲方对不符合保密条款的事项提出整改要求时，乙方应及时自查自纠、配合查处，不得拖延隐瞒。

6. 乙方不得进行超出甲方允许范围的工作，不得进入未授权的计算机网络和信息系统，或者使用未授权的计算机网络和信息系统资源。

7. 乙方未经甲方允许，不得对计算机信息网络和信息系统功能、存储或者传输的数据和应用程序进行删除、修改和传播。

8. 乙方不得在甲方网络和信息系统中加载与实施或服务内容无关的数据和程序，不得安装、测试具有探测、扫描、攻击性的程序，不得设置后门和恶意代码。

9. 乙方不得将自带移动设备和移动存储介质接入甲方的生产控制大区；应进行病毒查杀后经过甲方许可方可接入到管理大区，确保不存在恶意代码、病毒及后门等。

10. 乙方如果发现甲方信息系统存在网络安全隐患，或者因自己过失导致存在网络安全隐患，应保存相关日志，并立即向甲方报告。

11. 为甲方提供产品和服务，或因身份、职务、职业或专业技术关系而知悉甲方网络安全秘密的乙方机构和人员（包括但不限于乙方工作人员、代理人 and 雇员等）均应遵守本条有关乙方义务的约定，其行为视为乙方行为。

12. 甲方向乙方提供的相关系统登录用户名和密码，乙方仅用于主合同实施所需使用，不得擅自做其他用途或泄露给第三方。主合同履行完毕后，甲方将收回相关用户名及密码。

13. 乙方及其工作人员、雇员、代理人如违反本条义务的，应承担本协议第四条

规定的违约责任。

第三条 保密义务的终止

乙方应承担的保密义务期限为设备及系统的全生命周期，乙方是否完成合同义务、甲乙双方签订的合同是否履行完毕，均不影响其网络安全保密义务的承担。

第四条 违约责任

1. 乙方违反本协议约定的网络安全保密义务的，应向甲方支付主合同总价 10%违约金，并赔偿甲方损失。甲方损失包括实际损失，以及为处理该事件所支出的费用（包括但不限于律师费、公证费、取证费及甲方因索赔产生的一切费用）。

2. 主合同期内，若乙方违反本协议，甲方有权单方解除与乙方签署的主合同。

3. 因乙方恶意泄露网络安全秘密，给甲方造成严重后果的，甲方可通过法律手段追究其侵权责任，直至追究其刑事责任。

4. 乙方对乙方任何工作人员、代理人和雇员违反本协议的行为负责。上述人员违反本协议约定，甲方有权直接要求乙方承担违约责任。

第五条 争议解决方法

因执行本协议而发生纠纷的，按主合同约定的争议解决方法执行。

第六条 双方确认

1. 在签署本协议前，双方已经详细审阅了协议的内容，并完全了解协议各条款的法律含义。

2. 乙方只能为实现主合同目的使用甲方网络安全秘密，不作任何他用。

3. 主合同价款已包含保密义务人的保密费，此处不再重复支付。

第七条 协议的效力和变更

1. 本协议作为附件与主合同同步审批，经双方签字盖章后生效。

2. 除非甲方书面通知乙方解除保密义务，乙方的保密义务永久持续有效，不因主合同效力终止而终止；此前签署的其他有关保密协议不因本协议生效而发生任何效力变化。

3. 本协议的任何修改必须经过双方的书面同意，并签署相关补充协议，与本协议具有同等法律效力。

甲方（公章或合同专用章）： 乙方（公章或合同专用章）：

法定代表人或授权代表：

法定代表人或授权代表：

签署时间：

签署时间：

附件5.

廉洁协议

甲方（甲方）：_____

乙方（乙方）：_____

为了防范和控制_____合同（合同编号：_____）商订及履行过程中的廉洁风险，维护正常的市场秩序和双方的合法权益，根据反腐倡廉相关规定，经双方商议，特签订本协议。

一、甲乙双方责任

1. 严格遵守国家的法律法规和廉洁从业有关规定。
2. 坚持公开、公正、诚信、透明的原则（国家秘密、商业秘密和合同文件另有规定的除外），不得损害国家、集体和双方的正当利益。
3. 定期开展党风廉政宣传教育活动，提高从业人员的廉洁意识。
4. 规范招标及采购管理，加强廉洁风险防范。
5. 开展多种形式的监督检查。
6. 发生涉及本项目的不廉洁问题，及时按规定向双方纪检监察部门或司法机关举报或通报，并积极配合查处。

二、甲方人员义务

1. 不得索取或接受乙方提供的利益和方便。
 - （1）不得索取或接受乙方的礼品、礼金、有价证券、支付凭证和商业预付卡等（以下简称礼品礼金）；
 - （2）不得参加乙方安排的宴请和娱乐活动；不得接受乙方提供的通讯工具、交通工具及其他服务；
 - （3）不得在个人住房装修、婚丧嫁娶、配偶、子女和其他亲属就业、旅游等事宜中索取或接受乙方提供的利益和便利；不得在乙方报销任何应由甲方负担或支付的费用；
2. 不得利用职权从事各种有偿中介活动，不得营私舞弊。
3. 甲方人员的配偶、子女、近亲属不得从事与甲方项目有关的物资供应、工程分包、劳务等经济活动。

4. 不得违反规定向乙方推荐分包商或供应商。

5. 不得有其他不廉洁行为。

三、乙方人员义务

1. 不得以任何形式向甲方及相关人员输送利益和方便。

(1) 不得向甲方及相关人员行贿或馈赠礼品礼金；

(2) 不得向甲方及相关人员提供宴请和娱乐活动；不得为其购置或提供通讯工具、交通工具及其他服务；

(3) 不得为甲方及相关人员在住房装修、婚丧嫁娶、配偶、子女和其他亲属就业、旅游等事宜中提供利益和便利；不得以任何名义报销应由甲方及相关人员负担或支付的费用。

2. 不得有其他不廉洁行为。

3. 积极支持配合甲方调查问题，不得隐瞒、袒护甲方及相关人员的不廉洁问题。

四、责任追究

1. 按照国家、上级机关和甲乙双方的有关制度和规定，以甲方为主、乙方配合，追究涉及本项目的不廉洁问题。

2. 建立廉洁违约金制度。廉洁违约金的额度为合同总额的 1%（不超过 50 万元）。如违反本协议，根据情节、损失和后果按以下规定在合同支付款中进行扣减。

(1) 造成直接损失或不良后果，情节较轻的，扣除 10%-40% 廉洁违约金；

(2) 情节较重的，扣除 50% 廉洁违约金；

(3) 情节严重的，扣除 100% 廉洁违约金。

3. 廉洁违约金的扣减：由合同管理单位根据纪检监察部门的处罚意见，与合同进度款的结算同步进行。

4. 对积极配合甲方调查，并确有立功表现或从轻、减轻违纪违规情节的，可根据相关规定履行审批手续后酌情减免处罚。

5. 上述处罚的同时，甲方可按照公司有关规定另行给予乙方暂停合同履行、降低信用评级、禁止参加甲方其他项目等处理。

6. 甲方违反本协议，影响乙方履行合同并造成损失的，甲方应承担赔偿责任。

五、监督执行

1. 本协议作为项目合同的附件，由甲乙双方纪检监察部门联合监督执行。

2. 甲方电话_____；乙方电话_____。

六、其他

1. 因执行本协议所发生的有关争议，适用主合同争议解决条款。

2. 本协议签订份数与主合同一致。

3. 本协议作为附件与主合同同步审批，主合同签订后即生效。

甲方（公章或合同专用章）： 乙方（公章或合同专用章）：

法定代表人或授权代表： 法定代表人或授权代表：

签署时间： 签署时间：

附件 6.

保密协议

甲方：重庆长电渝电力工程有限公司

乙方：_____

因乙方为甲方提供服务，已经（或将要）知悉甲方的保密信息。为了明确乙方的保密义务，有效保护甲方的保密信息，防止该保密信息被公开披露或以任何形式泄露，根据《中华人民共和国民法典》《中华人民共和国反不正当竞争法》等法律法规，甲乙双方本着平等、自愿、公平和诚实信用的原则签订本保密协议，构成主合同的组成部分。

第一条 保密信息的定义

1. 本协议所指“保密信息”，是指甲方或其关联公司所持有的，甲方以口头、书面、数码或其他形式向乙方提供或透露的图像资料、年度大事件、商业机密、贸易机密、操作信息、技术信息、商务或财务相关的信息以及其他不被公开知道的信息，包括但不限于：

（1）发展规划策略、市场营销计划、商务信息、商业机密等。

（2）客户名称及清单、客户的详细资料、销售目标、销售统计表、销售办法、市场份额统计表、价格策略、市场研究报告、广告、其他促销资料等。

（3）财务信息、开户银行资料、组织架构、股东资料、投资背景等。

（4）公司知识产权（不论是公司独自拥有的或是和其他方共同拥有的，亦不论是现有的或将来开拓发展的），包括但不限于软件及相关程序、资料的著作权，及非专利技术、商业秘密，安装及维护方面的信息等。

（5）将来的资金项目、营业发展计划、商业关系和谈判等。

(6) 乙方在本合作业务过程中知悉的甲方尚未公开披露的其他信息。

2. 甲方依照法律规定（如在缔约过程中知悉其他相对人的保密信息）和在有关协议的约定（如技术合同）中对外承担保密义务的事项，也属本保密协议所称保密信息的范畴。

3. 本协议之签订可认为甲方已对公司的保密信息采取了合理的保密措施。

第二条 保密义务人

保密义务人是指为甲方提供相关服务，或因身份、职务、职业或专业技术关系等而知悉甲方保密信息的乙方、乙方机构或人员。

第三条 保密义务人的保密义务

1. 保密义务人应采取完善措施对甲方保密信息加以保护，并严格保守，保证不被披露或使用，包括意外或过失，即使这些信息可能是全部由保密义务人本人因工作而构思或取得的。乙方应确保知悉甲方保密信息的乙方人员（包括该人员在退出项目或离职之后）遵守本协议约定的保密义务。

2. 在服务关系存续期间，保密义务人未经授权，不得擅自披露、使用保密信息、制造再现保密信息的器材、取走与保密信息有关的物件；不得刺探与合同约定的乙方工作无关的保密信息；不得直接或间接地向乙方内部、外部的无关人员泄露；不得向不承担保密义务的任何第三人披露甲方的保密信息；不得允许（出借、赠与、出租、转让等处分甲方保密信息的行为皆属于“允许”）或协助不承担保密义务的任何第三人使用甲方的保密信息；不得复制或公开包含甲方保密信息的文件或文件副本；对因工作所保管、接触的有关甲方保密信息的文件应妥善对待，未经许可不得超出工作范围使用。

3. 如果发现甲方保密信息被泄露或者自己过失泄露保密信息，应当采取有效措施防止泄密进一步扩大，并及时向甲方报告。

4. 服务关系结束后，保密义务人应将与工作有关的技术资料、试验设备、试验材

料、客户名单等以及所有乙方保留或控制的该文件及资料的复印件、摘要等交还甲方；同时，乙方应销毁与已交回保密信息有关的任何文件和资料，不得保留复印件或以任何方式留存信息。

乙方如违反本条规定的，应承担本协议第五条约定的违约责任。

第四条 保密义务的终止

保密义务人应承担保密义务直至该保密信息已通过合法途径进入公共领域，成为公开信息；乙方是否完成合同义务、甲乙双方签订的合同是否履行完毕，均不影响其保密义务的承担。

第五条 违约责任

1. 乙方违反本协议约定的保密义务的，应向甲方支付主合同总价【10%-20%】违约金，并赔偿甲方损失。甲方损失包括实际损失，以及为处理该事件所支出的费用（包括但不限于律师费、公证费、取证费及甲方因索赔产生的一切费用）。

2. 主合同期内，若乙方违反本协议，甲方有权单方解除与乙方签署的主合同。

3. 因乙方恶意泄露保密信息给公司造成严重后果的，甲方将通过法律手段追究其侵权责任，直至追究其刑事责任。

4. 乙方对乙方任何工作人员、代理人 and 雇员违反本协议的作为或不作为负责。上述人员违反本协议约定，甲方有权直接要求乙方承担违约责任。

第六条 争议解决方法

因执行本协议而发生纠纷的，按主合同约定的争议解决方法执行。

第七条 双方确认

1. 在签署本协议前，双方已经详细审阅了协议的内容，并完全了解协议各条款的法律含义。

2. 保密义务人只能为实现主合同目的使用甲方保密信息，不作任何他用。

3. 主合同价款已包含保密义务人的保密费，此处不再重复支付。

第八条 协议的效力和变更

1. 本协议作为附件与主合同同步审批，经双方签字盖章后生效。
2. 除非甲方书面通知乙方解除保密义务，或出现法律规定、本协议约定的情形，乙方的保密义务永久持续有效，不因主合同效力终止而终止；此前签署的其他有关保密协议不因本协议生效而发生任何效力变化。
3. 本协议的任何修改必须经过双方的书面同意，并签署相关补充协议，与本协议具有同等法律效力。

甲方（公章或合同专用章）： 乙方（公章或合同专用章）：

法定代表人或授权代表： 法定代表人或授权代表：

签署时间： 签署时间：

合规承诺函

(采购人):

为与贵司建立互惠互利的良好商业合作关系，全面响应贵司合规要求，承诺人（商业合作伙伴名称）特作出以下承诺：

一、承诺人在_____过程中，严格遵守中国、业务所在国，以及依据长臂管辖原则等可以适用的法律、法规、行业管理规范、业务监管要求、条例和惯例等，包括但不限于反欺诈、反贿赂、反垄断、反不正当竞争、外汇管制、反洗钱、知识产权保护、职业健康安全、劳工保护、环境保护、数据安全、个人信息保护和国家安全等方面的任何规定。承诺人未实施且不会实施任何可能使贵司承担法律责任的行为。

二、承诺人不向贵司及员工实施任何形式的贿赂行为，即以影响另一方与贵司业务相关的行为或决定为目的，直接或间接地提供、给予、接受或要求任何有价值物或其他好处。

三、承诺人不以影响商业决策或获取不正当利益为目的，直接或间接向政府官员、其他商业主体等任何人士或相关方提供、支付、给予、要求或承诺提供、支付、给予任何形式的贿赂、回扣及特殊待遇。

四、承诺人将全面协助和配合贵司的所有商业行为符合合规要求，并维持准确的财务记录，真实准确地在财务账簿中反映其与_____有关的所有费用支出，并妥善保留相关财务凭证。

五、贵司及贵司聘请的第三方有权对承诺人遵守本承诺函的情况开展审计。承诺人同意配合贵司的合规审计，包括配合就相关事项进行解释说明、贵司或贵司聘请的第三方提供与商业事项相关的往来文件、交易记录、财务账簿及其他会计凭证等资料。若相关的财务记录不准确，或者出现拒绝提供、隐瞒或提供虚假信息，或者存在行贿受贿、虚假报销等违规行为的嫌疑时，贵司均有权单方面以书面通知形式终止该商业事项。

六、承诺人在开展与贵司相关的业务中，如果需要再次聘请次级代理商、分销商、

分包商或其他商业伙伴，应尽最大努力对业务中再聘请的第三方进行合规管理。

七、承诺人所提供的任何声明、信息和业务陈述都是准确真实的。若相关信息存在任何更新或变化，将及时书面通知贵司，并根据贵司要求提供更新后的相关材料。

八、承诺人违反以上承诺，应承担违约责任，包括但不限于赔偿贵司因此产生的全部损失。

特此承诺。

承诺人：_____（公章）

法定代表人或其委托代理人签字：

年 月 日

第四章 网络安全防护设计方案

1 概述

1.1 方案背景

随着国家信息化发展战略的不断推进，信息资源已经成为代表国家综合国力的战略资源。信息安全是保障国家主权、政治、经济、国防、社会安全和公民合法权益的重要保证。近年来国家高度重视网络安全工作。

电力行业作为国民经济的基础性、战略性产业，其网络安全直接关系到社会秩序、公共利益乃至国家安全。国家能源局修订印发的《电力行业网络安全等级保护管理办法》明确规定，电力行业网络根据重要程度及破坏后危害程度划分为五个安全保护等级，网络受到破坏后，会对社会秩序和公共利益造成危害，或者对国家安全造成危害，要求电力企业必须严格落实等级保护要求，新建的电力网络应当在通过等级保护测评后投入运行，且定时开展一次等级保护测评和自查工作，筑牢电力行业网络安全屏障。同时，《电力监控系统安全防护规定》明确电力监控系统需实施分区防护，进一步细化了电力行业网络安全防护的具体要求，为电力项目网络安全建设提供了行业规范指引。

鱼背山科研成果验证基地光伏电站现需接入到调度网络，其涉及光伏发电、能源调度、设备监控等核心业务，其网络系统承载着电站的运行数据、设备管控信息等关键内容，直接关系到调度网络的安全稳定运行，以及区域能源供应的可靠性，一旦网络系统遭到破坏、数据泄露或功能丧失，将对电力调度网络的运行和社会公共利益造成危害，需进行全面的网络安全防护建设。

1.2 建设目标

1.2.1 满足网络安全等保合规要求

严格对标国家网络安全等级保护制度 2.0 标准，基于信息系统的安全保护等级科学规划建设路径。从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等维度，全面梳理等级保护的基本目标、控制项和控制点，确保整体支撑体系框架及技术方法与国家政策、标准精准契合。通过对鱼背山科研成果验证基地光伏电站的合规建设，使信息系统在安全管理制度、技术防护措施等方面达到国家法定要求，规避法律风险，为业务开展筑牢安全合规基石。

1.2.2 构建电站保护纵深防御体系

基于等级保护 2.0 框架的分区域防护原则，打造“一个中心管理下的三重防护”纵深防御体系。以安全管理中心为核心，统筹协调安全策略、安全运维、安全审计等工作；构建安全区域边界、安全计算环境、安全通信网络的三重防护屏障。在事前，部署高级威胁监测设备，通过对

流量的深度解析，实时监测网络流量，主动预警潜在安全威胁；事中，强化防火墙、入侵检测、恶意代码防范等安全设备能力，建立动态访问控制机制，及时阻断恶意攻击行为；事后，完善审计日志留存与分析系统，还原攻击路径，形成完整的安全事件闭环管理。通过该体系，实现覆盖攻击前预警、攻击中防御、攻击后追溯全流程的安全防护能力，保障信息系统持续、稳定、安全运行。

1.2.3 构建自适应安全综合防控体系

深度融合安全技术体系、安全管理体系、安全运营体系。秉持“实战化、体系化、常态化”的建设思路，构建集“动态防御、主动防御、纵深防御、精准防护、整体防控”于一体的自适应网络安全综合防控体系。

1.3 编制依据

- 《中华人民共和国网络安全法》
- 《中华人民共和国计算机信息系统安全保护条例》（国务院令[1994]147号）
- 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
- 《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）
- 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
- 《信息安全技术 网络安全等级保护安全技术要求》（GB/T 25070-2019）
- 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）
- 《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）
- 《电力监控系统安全防护规定》（国家发改委〔2024〕27号）
- 《国家能源局关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范》（国能安全〔2015〕36号）

1.4 设计原则

- 安全合规原则

建设过程及成果完全依据核心业务信息系统特点、国家政策标准重要指导，建设完毕后符合监管单位、测评单位检查要求。

- 降低风险原则

合理分区分域，加强区域边界风险控制，构建纵深防御机制，降低系统风险。

- 分权制衡原则

合理划分权限，加强权限管控，构建有制约、有监督的权限管控机制，保障信息系统安全。

- 利于扩展原则

充分考虑到后期的业务拓展与新型系统威胁趋势，从分预留相应的可拓展接口，利于系统的功能、性能扩充。

- 适度安全原则

安全保护应适度，各个域的保护水平应根据其重要级别和业务功能来确定，根据应用、系统、网络和机房的具体情况来设计，任何信息系统都不能做到绝对的安全，过多的安全要求必将造成易用性降低和运行的复杂性，因此要在安全需求、安全风险和易用性之间进行平衡和折中。

- 技术与管理并重原则

在安全系统建设过程中，技术与管理都是安全体系的重要组成部分，疏忽哪方面的工作都会带来安全风险及安全隐患，因此两方面工作需要同步建设。

- 安全可控原则

在建设过程中尽可能多的采用自主创新、自主可控的技术、设备和服务。

- 兼容 IPv6 原则

网络安全等级保护应用建设中安全设备应满足当前环境对 IPv6 应用建设需求，尽可能采用支持且满足 IPv6 协议的设备。

1.5 项目范围

本期建设，主要依据“等保 2.0”第二级及电力行业相关标准要求，对鱼背山科研成果验证基地光伏电站进行网络安全防护设计。

2 设计需求分析

鱼背山科研成果验证基地光伏电站系统数据已经成功接入水风光联合控制系统，现需要将其数据接入到电力调度系统中，为保障调度网络的安全性，光伏电站部分需要进行网络安全加固后接入调度，同时确保光伏电站系统满足通过等保二级测评的技术要求。

2.1 安全技术层面需求

2.1.1 安全物理环境需求

物理环境安全是整个网络系统安全的前提，物理安全包括机房电源安全、电磁兼容性安全、环境安全、设备安全、防雷接地、记录介质安全等。网络系统的建设属于弱电工程，耐压值很低。因此须优先保护人和网络设备不受电、火灾和雷击的侵害，确保布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的安全距离；满足布线系统和绝缘线、裸体线以及接地与焊接的安全需求；建设防雷系统，确保建筑物防雷、计算机及其他弱电耐压设备的防雷。本期安全物理环境的需求主要从机房工程、专用链路两个方面上来体现。

表 4 物理安全与实现方式

序号	具体实现	功能描述	安全属性	部署方式
1	机房工程	安全设备中心电源安全、电磁兼容性安全、环境安全、设备安全、防雷接地、记录介质安全	保密性 可控性	机房重地与普通办公楼层之间
2	专用链路	电磁兼容性安全、环境安全、设备安全	保密性 可控性	运营商侧 自建链路

2.1.2 安全通信网络需求

在数据传输的完整性、保密性方面，采用密码技术或其他有效措施，确保系统管理数据、鉴别信息和重要业务数据在传输过程中的完整性、保密性。

采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障，主要网络设备、通信线路和数据处理系统硬件冗余，保证系统的高可用性。

2.1.3 安全区域边界需求

合理划分安全域，防范来自低安全级别区域的安全威胁，同时尽可能将安全风险（如黑客攻击或病毒蠕虫传播）限制在较小的、不太重要的局部区域范围内。详细需求如下：

- 在安全子区域边界采用防火墙进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保网络和信息自身的安全。
- 在安全域出口分别部署多功能的安全网关设备，对进出网络及访问重要服务器系统的数据流进行黑客攻击、蠕虫、木马、病毒等非法流量的检测和拦截，并提供适当的日志和报警机制，

确保通信网络和服务器系统不会因为外界攻击而无法正常工作。

- 准确监测重要安全域的网络异常流量，实时、自动的阻断各类攻击性的流量，并及时告警。
- 在网络接入边界采用防火墙进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保网络和信息系统的自身安全。
- 对网络流量进行抓包分析，捕获 APT 攻击行为，实现 APT 预警。并对文件进行检测，发现文件中的恶意代码。
- 建立严密的病毒防范体系，对所有服务器和终端系统进行病毒监测，防止病毒在网络内部的传播。
- 有效隔离内外网，允许合法用户的访问以及限制其正常的访问，禁止非法用户的试图访问。

2.1.4 安全计算环境需求

计算环境为网络系统的稳定运行提供核心动力，要将安全风险控制在最小的范围之内。详细需求如下：

- 实现对数据库访问的详细记录、监测访问行为的合规性，针对违规操作、异常访问等及时发出告警，将安全风险控制在最小的范围之内。
- 建立集非法接入监控、非法外联监控、用户行为审计、补丁管理、系统监管、安全防护等功能于一体的终端安全防护体系。

2.1.5 安全管理中心需求

安全管理中心是进行集中管控的区域，需集中监控各种网络安全资源、统一管理安全策略、全面审计用户以及操作行为、联动各项安全能力，将网络安全管理工作化繁为简。

详细需求如下：

- 需对系统管理维护人员和业务操作人员进行统一的账号、认证和授权管理，并需要强化身份认证机制。
- 需统一审计运维操作，拦截运维人员对目标设备的非法访问、操作行为。
- 需进行日志记录的统一收集、存储、分析、查询、审计和报表输出。
- 需对来自业务应用系统和数据库系统用户的网络访问行为和网络传输内容进行记录，为安全事件的追踪与调查取证提供翔实缜密的数据支持。

2.2 安全管理层面需求

2.2.1 安全管理组织需求

现有的机构设置、岗位设定、人员配备等不能完全满足对信息系统的的海关管理需求，在很大程度上制约了信息安全体系建设的的发展，需建立健全安全管理组织。详细需求如下：

- 需建立全网统一的安全管理组织机构，专门负责信息系统的安全管理和监督。
- 需制定符合业务系统业务特点的人员安全管理条例。
- 需对 IT 使用人员和运维管理人员进行安全意识和安全技能培训，提高自身的安全管理水平。

2.2.2 安全管理制度需求

当前安全管理制度建设还不完善，需依据国家网络安全相关政策、标准、规范，制定、修订并落实与等级保护对象安全管理相配套的、包括等级保护对象的建设、开发、运行、维护、升级和改造等各个阶段和环节所应遵循的行为规范和操作规程。

缺乏健全的制度策略体系。详细需求如下：

- 需制定符合国家和行业监管部门安全管理要求，并符合业务系统自身特点的安全管理制度，保证信息系统的安全运行。
- 需规范安全管理流程，加大安全管理制度的执行力度，以确保整个网络系统的安全管理处于较高的水平。
- 需要建立安全应急预案并定期进行演练、审查和更新。

2.2.3 安全运营需求

当前还缺乏一整套的安全服务保障体系。需通过流程化、规范的手段，有序开展安全工作，构建持续安全运营能力，保障业务系统的安全稳定运行。详细需求如下：

需要由专业的安全服务人员为业务系统提供安全事件的应急响应服务，一旦发生安全问题，信息系统管理员能够在最短的时间内通知到安全专家并及时进行问题的解决，以尽可能缩小安全事件的影响范围和程度，并尽快恢复信息系统的正常运行。

需要提供专门的安全服务团队进行安全培训等安全专项服务，通过这些安全人员的参与，形成有效的安全运营防护体系。

3 总体设计思路

3.1 网络安全拓扑

整体项目架构如上图：

1、鱼背山科研成果验证基地光伏电站已经建设完毕，现已经正常接入到水风光联合控制中；

2、光伏电站通过现有远动装置或数据采集服务器把电站监控运行数据接入到电力调度系统中，远动装置或数据采集服务器即为光伏电站核心数据网络的边界防护设备，同时在安全 I 区和安全 II 区的接入边界分别部署纵向加密装置、路由器等网络设备接入电力调度系统中；

3、在光伏电站安全 I 区旁路部署相关交换机、安全及审计设备，实时监控数据安全，保障光伏电站数据安全接入到电力调度网中：

部署 APT 预警平台、入侵检测和恶意代码防范设备，实现整个系统流量安全监测、威胁分析及防护；

部署堡垒机，实现运维账号管理，集中访问控制及安全审计；

部署 II 型网络安全监测装置，实现对本地电力监控系统内监测对象的数据采集与处理，同时把处理的结果上送至调度机构部署的网络安全管理平台。对用户的各类日志进行综合审计分析，通过对访问记录的深度分析，发掘出潜在的威胁，起到追根溯源的目的，并且记录服务器返回的内容，便于取证式分析；

部署数据库审计系统，通过数据库流量的采集、分析、识别，具备全面的数据库访问审计能力；

同时，相关采集服务器和 workstation 部署防病毒系统，实现病毒防护及终端管理；

4、光伏电站安全 II 区的光功率预测设备需要接入到互联网，在边界接入区域部署反向隔离装置及防火墙，并在防火墙上增加入侵防御和防病毒等安全防护模块，实施对互联网数据进行安全检测及防护，保障互联网接入区域安全性；

5、本次部署的相关的安全及审计设备需支持冗余设计，多接口可同时审计光伏电站安全 I 区和安全 II 区数据，安全 II 区数据通过新增交换机镜像数据后发送至 I 区安全管理中心进行监测及审计；

6、考虑到全网设备的时间同步，导致日志审计及事件溯源存在时间偏差风险。在安全 II 区新增一套 NTP 时间对时装置（支持北斗/GPS 双模授时），精度满足电力系统要求（毫秒级）。对时装置应为所有网络设备、安全设备、服务器提供统一授时，并具备时钟源切换功能。

7、本次通讯网络中的 SDH 设备 ZXMP S330 缺少接入端口，需要增加相应的通讯以太网板卡。

4 详细设计思路

4.1 安全技术体系

4.1.1 安全物理环境

安全物理环境是支撑整个网络应用系统的基石，其作为网络安全技术体系建设的重要组成部分须依据等级保护基本要求中对物理安全的有关要求，并结合信息化大集中、大整合、高共享的建设实际，不断扩展和变化，以满足信息化建设对基础设施保障和设备、数据安全的需求。

安全物理环境体系建设规划与应用的发展有着紧密的联系，其设计方向必须紧贴应用发展的实际需求。在基础设施方面建设机房的防雷击、防火、防水、防潮、防静电、动力系统、动环监控系统，电磁防护系统，使应用部署不再受到机房、功能区域的限制，消除物理安全风险隐患，让系统的建设更加灵活且具有高度的可扩展性。在物理安保方面进一步加强对人员的管控，通过整合现有安保资源，形成多元化的安保防控一体化构建，达到对资产的全面管理和安全防护。目前鱼背山科研成果验证基地光伏电站机房已经建设完毕，物理环境已基本符合等保 2.0 要求，本设计方案不做赘述。

4.1.2 安全通信网络

网络通信过程中的任一环节遭受攻击，都将对数据安全构成严重影响和威胁。因此结合等级保护安全通信网络控制点要求、等级保护安全设计技术要求，从网络架构、通信传输、可信验证三方面进行安全通信网络建设。

4.1.2.1 纵向加密装置

【部署目的】

纵向加密装置通过双向身份认证与数据加密传输，确保调度指令与遥测数据在传输过程中的机密性、完整性及真实性；同时，通过基于五元组（源/目的 IP、端口、协议）的策略控制，实现对上下行数据流的精细化访问控制，仅放行合法的业务数据，阻断非法访问与恶意流量。

【部署方式】

分别在光伏电站安全 I 区、安全 II 区至调度网方向串接一台部署纵向加密设备，从而保证数据通信的机密性、完整性及真实性；并且作为边界第一道防线，实现网络访问控制，有效防止非法访问或未授权访问。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.2 安全通信网络

8.1.2.1 网络架构

本项要求包括：

- b) 应保证网络各个部分的带宽满足业务高峰期需要；
- c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

d) 应避免将重要网络区域部署在边界处,重要网络区域与其他网络区域之间应采取可靠的技术隔离手段;

【部署效果】

光伏电站出口部署纵向加密装置,保障电站与调度之间的所有指令、数据均经加密传输,即使被截获也无法解密,杜绝了网络窃听风险;通过密码校验机制,确保调度指令在传输中不被恶意篡改或伪造,保障操作的原始性;基于策略的精细化访问控制,只放行允许的业务数据流,非法访问被直接阻断,安全策略执行情况清晰可审计。

4.1.2.2 下一代防火墙

【部署目的】

防火墙是目前技术最成熟的网络安全产品,通常使用安全区的边界,在边界处部署防火墙,将内部网和外部不信任网络、内部网络中主要的应用服务器和内部其它网段用防火墙隔离保护,以实现内部网以及主机系统的访问控制和边界安全的集中管理。同时,出口防火墙上配置 NAT,实现内网用户访问外网,内网服务器对公网提供服务。

【部署方式】

在安全 II 区光功率预测设备至互联网边界部署下一代防火墙设备,从而保证通信的连续性和可靠性;并且作为边界第一道防线,实现网络访问控制,有效防止非法访问或未授权访问。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.2 安全通信网络

8.1.2.1 网络架构

本项要求包括:

- b) 应保证网络各个部分的带宽满足业务高峰期需要;
- c) 应划分不同的网络区域,并按照方便管理和控制的原则为各网络区域分配地址;
- d) 应避免将重要网络区域部署在边界处,重要网络区域与其他网络区域之间应采取可靠的技术隔离手段;

【部署效果】

下一代防火墙秉持“持续边界安全态势改善”的理念,以用户为核心,以边界、应用、威胁、权限为防护对象,构建以资产为视角的可持续智能安全运营防护体系,集传统防火墙、入侵防御、防病毒、上网行为管控、VPN、威胁情报等安全模块于一体,同时可联合态势感知、EDR 等产品进行一体化网络安全建设。

4.1.2.3 反向隔离装置

【部署目的】

反向隔离装置是在绝对保障生产控制区域(内网)安全的前提下,单向接收来自管理信息区

域（外网）的调度指令与数据。它通过物理单向传输技术，彻底阻断从外网向内网的网络攻击路径，既实现了数据从低密级网络传输到高密级网络的应用需求，又确保核心控制系统在接收外部信息时不被恶意入侵，是国家电力监控系统安全防护体系中强制性的“安全门禁”。

【部署方式】

在 II 区的光功率预测设备与生产控制区域边界部署反向隔离装置，保证光功率预测设备与生产控制区域通信的可靠性；采用单向通信传输系统，数据从低密级网络传输到高密级网络，无双向数据传输通道，在物理链路层杜绝信息的反向传输，物理硬件上彻底保证了内网机密数据无法泄露到外网。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.2 安全通信网络

8.1.2.1 网络架构

本项要求包括：

- c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
- d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

【部署效果】

- **安全接收:**外网的调度指令（如 AGC/AVC 调节）能经签名验证、内容过滤后安全传入内网控制系统；
- **彻底阻断:**因采用专用硬件和单向通道技术，任何从外网发起的网络攻击、病毒传播或非法访问均无法穿透至内网；
- **强制合规:**满足国家电力监控系统安全防护“横向隔离”的刚性要求，确保电站并网运行合法合规。

简言之，该装置既打通了必要的遥控指令通道，又确保生产控制区“只进不出、外网不可达”，有效保障了电力生产系统的网络安全。

4.1.3 安全区域边界

安全区域边界是指系统的安全计算环境边界，以及安全计算环境与安全通信网络之间的边界。依据等级保护安全通信网络控制点要求、等级保护安全设计技术要求，从边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等六个方面进行安全区域边界建设。

安全区域边界的建设过程中须充分考虑如下因素：

基于不同的网络安全域进行合理的边界划分，跨越边界的访问和数据流通过边界防火墙等设备进行访问控制和安全隔离。

在关键网络节点处检测、防止或限制从外部/内部发起的网络攻击、入侵行为，当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警，

同时进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

4.1.3.1 APT 预警平台

【部署目的】

随着越来越多的系统本身漏洞以及应用系统的漏洞被发现，以及攻击者的入侵方式更加隐蔽，新的攻击方式层出不穷，所以单纯的依靠防火墙已经无法完全防御不断变化的入侵攻击的发生。

传统的防火墙主要有以下的不足：

- 防火墙作为访问控制设备，无法检测或拦截嵌入到普通流量中的恶意攻击代码，比如针对具体应用或系统的攻击等。

- 防火墙无法基于应用层的智能协议识别实现对应用层的攻击防护。

因此，需要借助专业的入侵检测设备，实现对应用层攻击的检测与告警。

【部署方式】

在安全 I 区安全管理中心部署 APT 预警平台，设备通过旁路镜像方式接收进出的流量数据，从智能识别、环境感知、行为分析三方面加对应用协议、异常行为、恶意文件进行检测和防护，精确识别应用等各层面攻击，在不影响正常业务流量的前提下对攻击流量进行实时检测和告警。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.3.3 入侵防范

本项要求包括：

- a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
- b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
- d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。。

【部署效果】

APT 攻击检测系统针对弱点探测、渗透入侵、获取权限、命令与控制、数据盗取整个入侵攻击链中的攻击行为都具备检测能力。同时基于双向流量的解析机制，实时发现由外到内和由内到外的网络攻击行为。产品基于丰富的特征库、全面的检测策略、智能的机器学习、高效的沙箱动态分析、海量的威胁情报，能实时发现网络中发生的各种已知威胁和未知威胁，检测能力完整覆盖整个入侵攻击链。

4.1.3.2 入侵检测系统

【部署目的】

通过丰富的特征库、全面的检测策略、精准的深度分析模型，结合智能机器学习和云端威胁情报协同，实时发现用户网络中的各种已知威胁和未知威胁，检测能力可完整覆盖 APT 攻击链，同时对各类恶意代码攻击、远程控制、WEB 攻击、邮件攻击、漏洞利用、隧道通信等在内的二十余

种攻击类型检测，可发现 APT 武器库指纹、异常加密流量、防溯源 C&C 攻击、Oday 攻击等高级威胁，并通过可视化技术态势呈现网内威胁，支持联动明御数据包存储回溯系统，能组合实现流量回溯分析取证能力，帮助用户实时预警网络攻击事件，提升网络攻击感知能力，助力高级威胁溯源分析，满足等保合规建设，为用户提供更全面的安全保障。

【部署方式】

在安全 I 区安全管理中心部署入侵检测设备，实时发现用户网络中的各种已知威胁和未知威胁，能组合实现流量回溯分析取证能力，帮助用户实时预警网络攻击事件，提升网络攻击感知能力，助力高级威胁溯源分析，满足等保合规建设。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.3.3 入侵防范

本项要求包括：

- a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。
- b) 应在关键网络节点处检测和限制从内部发起的网络攻击行为。
- c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

【部署效果】

通过精准威胁识别，实时预警并多维度展示重点信息系统的网络攻击事件。能够完整、真实地还原网络和安全事件的原始场景。通过记录和存储数据包，为用户提供丰富的事后分析和审计取证能力。全量数据包存储回溯为网络和安全策略的制定提供了决策依据，通过对存储的数据包进行深入分析，用户可以发现系统中的漏洞和弱点，根据实际场景制定更有效的安全策略，确保网络和系统的稳定和可靠性。同时基于特征标签与上下文语义，实现实时切换场景分析相关数据，能够更准确地识别各种威胁。

4.1.3.3 恶意代码防范

【部署目的】

在网关或关键的网络节点主动清洗过滤掉应用数据中加载的病毒、木马、间谍软件等恶意代码，在病毒未进入内部网络感染内部主机和服务器之前进行阻断拦截，有效避免了病毒给用户带来的危害与影响。

【部署方式】

在安全 I 区安全管理中心部署恶意代码防范设备，实现在病毒未进入内部网络感染内部主机和服务器之前进行阻断拦截。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.3.4 恶意代码防护和垃圾邮件防范

- a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。

b)应在关键网络节点处对垃圾邮件进行检测和防护,并维护垃圾邮件防护机制的升级和更新。

【部署效果】

通过部署恶意代码防范设备,保障网络运行合规合法性,通过过滤病毒、木马、间谍软件或代码,避免内部设备或服务系统感染恶意病毒,防止恶意软件破坏篡改甚至恶意加密控制内部数据资料,保障了办公数据的完整性、可靠性并有效避免了恶意勒索事件的发生。

4.1.4 安全计算环境

依据网络安全等级保护安全计算环境控制点要求,同时结合网络安全等级保护安全设计技术要求,对等级保护对象安全计算环境进行设计,内容包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护十一个方面。计算环境作为系统内部防护的关键,承载着重要业务系统,以及用户重要数据的运行、存储和处理工作。

4.1.4.1 终端安全管理系统

【部署目的】

传统杀毒软件在应对勒索时的困境,单点能力无法应对勒索的分布式扩散,勒索病毒在局域网内大量扩散,对主机上安装的杀毒软件无法及时全部配置检测任务。杀毒软件无法处理未知的勒索病毒变种,勒索病毒变种繁多,杀毒软件依赖规则库,面对新型勒索病毒无法识别,只能任由其完成加密行为。

终端安全管理(EDR)的优势,防御已知和未知类型勒索病毒。面对使传统杀毒软件束手无策的未知类型勒索病毒,终端安全管理(EDR)采用诱饵引擎,在未知类型勒索病毒试图加密时发现并阻断其加密行为,有效守护主机安全。

【部署方式】

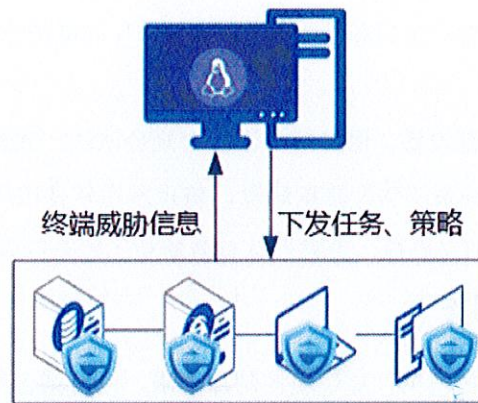
终端安全管理系统由管理控制中心和客户端组成,在服务器中部署终端管理系统的管理中心,主要功能为把所有客户端信息集中于一体,便于集中监管和配置安全策略,聚合客户端情报信息。

管理控制中心采用B/S架构,安装完成后,用户可以在任意与管理控制中心网络可达的计算机上访问管理控制中心的Web页面,对终端进行管控。

客户端软件是一个独立的本地可执行程序,安装在需要被管控的主机上,完成管理员通过管理控制中心下发的任务和策略。

在部署终端安全管理系统时,首先架设管理控制中心,然后在主机上安装客户端软件,即可实现管理控制中心与客户端的安全连接。

部署示意图:



【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8. 1. 4. 4 入侵防范

本项要求包括：

- a) 应遵循最小安装的原则，仅安装需要的组件和应用程序；
- b) 应关闭不需要的系统服务、默认共享和高危端口；
- c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
- d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统

设定要求；

- e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
- f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

8. 1. 4. 5 恶意代码防范

应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。

8. 1. 4. 6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，

并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果送至安全管理中心。

【部署效果】

● 恶意代码查杀

主机安全及管理系统具备恶意代码查杀功能，平台支持：Windows + x86/x64、Linux + x86/x64、Linux + MIPS 32/64 + 大小字节序、Linux + ARM 32/64、Unix + PowerPC、国产操作系统（Linux 家族） + 国产 CPU（x86/MIPS）。

支持多种压缩包、自解压包、符合文档、媒体文件、加密脚本、电子邮件、邮箱文件、可提取文档中嵌入的其它资源，如：宏、脚本、可执行程序等。

- 登录防护

使用操作系统本身公开的安全登录插件机制实现此功能，相较于传统的读取系统日志判断的方法，插件防护不会遗漏掉任何登录数据，更加安全。

可对系统账户登录进行细粒度的精准访问控制，支持对访问来源（账户、地理位置、远程 IP 或域名、远程计算机名）、访问时间的配置，并能实时阻断非法登录。触发登录防护后，自动联动添加微隔离规则。

可周期性执行弱口令检测或立即执行一次检测，检测字典包括常见弱口令、同用户名的口令和空口令。

- 进程防护

使用内核驱动技术，每当有进程启动时从操作系统内核中可以得到通知，获取到包括进程路径等一系列上下文信息后，可以根据运维人员设置的白名单直接拒绝或放行。支持仅记录模式、记录并阻断模式。

- 文件访问控制

使用系统文件过滤驱动技术，可细粒度审计文件创建、删除、写入、重命名等操作。

- 网络微隔离

内核级网络防火墙，网络驱动技术实现，不依赖系统自身的防火墙。

对不同的业务之间的流量进行精准识别、针对非法流量可以精准阻断，该功能广泛应用在云数据中心。

快捷操作直接输入需要关闭的端口或需要屏蔽的恶意 IP，自动生成隔离规则。

- 防端口扫描

在网络驱动中检查入站到本机的数据包，当某个 IP 在设置的时间周期内连接本地的不重复的端口数量达到一定次数时，将恶意探测 IP 锁定，防止其进一步获取终端敏感信息。可以查看并解除已临时锁定的 IP 清单。

- 违规外联防护

在网络驱动中检查本机的出站数据包，由内核中的快速匹配算法支持，即使有大量规则情况下，对网络性能的影响也可忽略不计。支持黑白名单两种模式，可手动添加或批量导入黑/白名单。

白名单：开启违规外联防护-白名单模式后，配置白名单 IP，除白名单 IP 以外连接记录或实时阻断。

黑名单：开启违规外联防护-黑名单模式后，配置黑名单 IP，连接黑名单内 IP 时记录或实时阻断。内置 10 万+威胁情报。

- 勒索防御

风险评估：检查系统中的弱口令、系统漏洞、恶意进程、高危端口等，给出感染勒索病毒的可能性。

勒索软件启动防护引擎：勒索病毒启动前会先通过杀毒引擎的扫描，针对已知的勒索病毒可

直接阻断其运行。

勒索软件加密防护引擎：通常勒索病毒加密文件之前都会执行例如遍历文件、读取文件、写入文件、删除或重命名文件等操作，主机安全及管理系统通过文件过滤驱动在随机位置创建诱饵文件，并通过算法使勒索病毒先遍历到诱饵文件，当内核检测到有程序对诱饵文件执行写入、重命名、删除任意一项操作时，会立即结束该程序，阻止其进一步运行。

- **挖矿防御**

挖矿病毒会大量消耗系统运行资源非法挖矿，挖矿防御功能通过对弱口令、系统漏洞、资源占用、恶意进程、DNS 历史查询和异常外联几项的检测，给出感染挖矿病毒的可能性，并通过主动防御机制，实时阻断挖矿病毒的运行。

4.1.4.2 数据库审计与风险控制系统

【部署目的】

随着信息技术的日新月异和网络信息系统应用的发展，政府、医疗网络技术的应用层次正在从传统的、小型业务系统逐渐向大型、关键业务系统扩展。信息安全是一个动态的过程，在为自身业务提供高效的网络运营平台同时，日趋复杂的 IT 业务系统与不同背景业务用户的行为也给网络带来潜在的威胁，特别是重要信息系统的数据库操作；如何有效监控数据库访问行为和敏感信息查询，准确把握数据库的安全状态，及时发现违反安全策略的事件并实时告警、记录，同时进行安全事件定位分析，事后追查取证，满足合规性审计要求，是单位需要解决的问题。数据库审计需要实现如下目标：

- **全面审计**

数据库访问审计日志的要素要尽量全面而详细、兼容各种数据库访问协议、支持三层数据库部署环境中的各种中间件，方便管理员全面掌握数据库访问情况。

- **准确定位**

能够准确识别具体的操作对象、能够准确地进行参数关联、能够准确地把后端数据库的 SQL 操作与前端 Web 应用的用户进行关联，便于管理员对所有的数据库访问进行精准定位、责任到人。

- **高效分析**

在海量日志中能够快速检索，帮助管理员快速检索、聚焦到关键的访问日志上。

- **风险告警**

在进行数据库访问审计的同时，能够有效识别针对数据库漏洞的各种攻击行为、有效区分 SQL 注入与正常的访问，全面降低数据库安全风险。

【部署方式】

在安全 I 区安全管理区部署一台数据库审计系统，本地机房的核心交换机镜像流量数至据库审计。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.4.3 安全审计

本项要求包括：

- a) 应启用安全审计功能,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计;
- b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息;

【部署效果】

数据库审计系统基于精细的数据库协议解析和专业的 SQL 语法、词法分析,通过数据库流量的采集、分析、识别,具备全面的数据库访问审计能力。根据 SQL 行为特征和关键词特征进行自动分类,系统访问 SQL 语句有效“归类”到几百个类别范围内,完成审计结果的高精确和高可用分析。从风险、语句和会话三个层面完成统计与检索查询功能,并支持多层级钻取,帮助用户高效的锁定风险目标。最终实现如下效果:

- 监控大规模数据泄漏和篡改

系统针对不同的数据库用户,提供敏感表的操作权限、访问行数和影响行数的监控,以及限制 NO WHERE 查询和更新操作的监控,从而避免大规模数据泄露和篡改。

- 语句管理与敏感数据

本系统通过 SQL 语法分析构建动态模型,形成信任语句和敏感语句管理,对信任语句正常执行,对敏感语句进行及时告警。

- 提供用户权限细粒度管理

本系统对于数据库用户提供比 DBMS 系统更详细的虚拟权限监控。

监控策略包括:用户+操作+对象+时间。

在操作中增加了 Update Nowhere、delete Nowhere 等高危操作;控规则中增加返回行数和影响行数因素。

- 全面精细审计分析

提供全面详细审计记录,告警审计和会话事件记录,并在此基础上实现了内容丰富的审计浏览、访问分析和问题追踪,提供实时访问首页统计图。

通过对捕获的 SQL 语句进行精细 SQL 语法分析,并根据 SQL 行为特征和关键词特征进行自动分类,系统访问 SQL 语句有效“归类”到几百个类别范围内,完成审计结果的高精确和高可用分析。

4.1.5 安全管理中心

依据网络安全等级保护安全管理中心控制点要求,同时结合网络安全等级保护安全设计技术要求,对等级保护对象安全管理中心进行设计,内容包括系统管理、审计管理、安全管理,集中管控四个方面。

在网络环境中建立安全管理中心是有效帮助管理人员实施安全措施的重要手段,是实现业务稳定运行、长治久安的基础。通过安全管理中心建设真正实现安全技术层面和管理层面的结合,全面提升用户网络安全保障能力。安全管理中心建设主要通过运维审计与风险控制系统、综合日

志审计分析平台、数据库审计与风险控制系统、安全分析与管理平台等监测管控机制实现。

4.1.5.1 II 型网络安全监测设备

【部署目的】

1、满足等保合规要求

目前国家的政策法规、行业标准等中都明确对日志审计提出了要求，日志审计已成为企业满足合规内控要求所必须的功能。例如：2016 年 11 月 7 日发布，2017 年 6 月 1 日起施行的《中华人民共和国网络安全法》中规定：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。《信息系统安全等级保护基本要求》中规定：二到四级需要对网络、主机、应用安全三部分进行日志审计。

2、满足业务需求

随着数字城管信息化的不断发展，信息化资产数量日趋增多、系统的关联性和复杂度不断增强，然而当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。日志审计能够更好地监控和保障信息系统运行，及时识别针对信息系统的入侵攻击、内部违规等信息，同时日志审计能够为安全事件的事后分析、调查取证提供必要的信息。

【部署方式】

在安全 I 区安全管理中心部署一台 II 型网络安全监测设备，对服务器、工作站、网络设备、安全防护设备、数据库等监测对象进行数据采集与处理，同时把处理的结果上送至调度网络安全管理平台。通过对访问记录的深度分析，发掘出潜在的威胁，起到追根溯源的目的，并且记录服务器返回的内容，便于取证式分析。

【政策规范】

《中华人民共和国网络安全法》

【第 21 条】 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；

第三点：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月

【部署效果】

➤ **全面的智能收集功能：**对服务器、工作站、网络设备、安全防护设备、数据库等监测对象进行数据采集，支持采集服务器、工作站的用户登录、操作信息、运行状态、移动存储设备接入、异常网络访问等事件信息；支持采集数据库的操作信息、运行状态等事件信息；支持采集安全防护设备的用户登录、配置变更、运行状态、安全事件信息等事件信息；

➤ **日志数据分析处理：**以分钟级统计周期，对重复出现的事件进行归并处理；根据参数配置，对采集到的 CPU 利用率、内存使用率、网口流量、用户登录失败、磁盘空间使用率等信息进行分析处理，根据处理结果决定是否形成新的上报事件；同时可以形成外设接入事件、用户登录

事件、危险操作事件、状态异常事件、异常网络访问事件等上传事件。

4.1.5.2 运维审计与风险控制系统

【部署目的】

构建一个强健的 IT 运维安全管理体系对网络安全的保障至关重要,对运维的安全性提出更高要求。面对日趋复杂的 IT 系统,不同背景的运维人员会给信息系统安全运行带来较大潜在风险,主要表现在:

- 账号管理无序,暗藏巨大风险
- 远程维护端口直接暴露在公网上
- 粗放式权限管理,安全性难以保证
- 设备自身日志粒度粗,难以有效定位安全事件
- 第三方代维人员带来安全隐患
- 传统网络安全审计系统已无法满足运维审计和管理的要求
- 面临法规遵从的压力

对于单位而言,需要有全面的技术手段对所有运维操作、流程进行审计,并控制不同运维人员的访问权限,从而实现平台的设备安全和运维安全。

【部署方式】

在安全 I 区安全管理中心部署一台运维审计系统,通过配置路由器或目标设备的访问控制策略,只允许集中运维审计的 IP 访问目标设备的运维、管理服务,建立基于唯一身份标识的实名制管理,统一账号管理策略,通过集中访问控制与授权,实现从登录到退出的全程操作行为审计,满足合规管理和审计要求。

【政策规范】

《信息安全技术网络安全等级保护基本要求》GB/T 22239-2019

8.1.4 安全计算环境

8.1.4.1 身份鉴别

本项要求包括:

- a) 应对登录的用户进行身份标识和鉴别,身份标识具有唯一性,身份鉴别信息具有复杂度要求并定期更换;
- b) 应具有登录失败处理功能,应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施;
- c) 当进行远程管理时,应采取必要措施防止鉴别信息在网络传输过程中被窃听;
- d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别,且其中一种鉴别技术至少应使用密码技术来实现。

【部署效果】

通过运维审计系统,可以达到如下效果:

- 集中账号管理

建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备、安全设备、数据库服务器等无缝连接。

- 集中访问控制

通过集中访问控制和细粒度的命令级授权策略，基于最小权限原则，实现集中有序的运维操作管理，让正确的人做正确的事。

- 集中安全审计

基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件的实时发现与预警。

4.2 安全管理体系

4.2.1 安全管理制度

依据网络安全等级保护安全管理制度控制点要求，同时结合网络安全等级保护安全设计技术要求，对等级保护对象安全管理制度进行设计，内容包括安全策略、管理制度、制定和发布，评审和修订四个方面。

根据基本要求制定各类管理规定、管理办法和暂行规定。应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等，对安全管理活动中各类管理内容建立安全管理制度。

指定或授权专门的部门或人员负责安全管理制度的制定，制定严格的发布流程，方式，范围等，且需要统一格式并进行有效版本控制；发布方式需要正式、有效并注明发布范围，对收发文进行登记。

成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；信息安全领导小组负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定，定期或不定期对安全管理制度进行评审和修订，修订不足及进行改进。

安全管理制度是对信息安全目标和工作原则的规定，其表现形式是一系列安全策略体系文件。安全管理制度是信息安全保障体系的核心，是信息安全管理、技术工作和运维工作的目标和依据。

具体安全管理制度参考以下内容建设：

1. 制定一套网络安全总体方针和安全策略，明确组织机构的总体目标、范围、原则和安全框架；
2. 制定一套安全管理制度，形成安全策略、管理制度、操作规程、记录表单四级管理制度体系；
3. 指派专人或者成立专门的小组负责制度的制定，安全管理制度要正式发布，并进行有效的版本控制；

4. 应定期对制度进行评审和修订，至少每年（建议）进行一次评审和修订；

4.2.2 安全管理机构

依据网络安全等级保护安全管理机构控制点要求，同时结合网络安全等级保护安全技术要求，对等级保护对象安全管理机构进行设计，内容包括岗位设置、人员配备、授权和审批、沟通和合作、审核和检查五个方面。

成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；

设置安全管理岗位，设立系统管理员、网络管理员、安全管理员等岗位，根据要求进行人员配备，配备专职安全员；成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

设置网络安全管理工作小组，并明确其职责。根据三权分立的原则设置工作岗位，设置三员角色，必须配备专职的安全管理员。

建立授权审批制度，明确职责和要求，重要活动逐级审批。并对审批事项进行定期审查。

建立定期协调会议制度，协调处理网络安全问题，加强与外部资源的沟通与合作，建立外部单位联系表，以便及时获取外部资源支持。

建立定期安全检测制度，检查内容覆盖技术、管理、策略等，并对检查结果进行分析，形成报告，并对结果进行通报。

具体安全管理机构参考以下内容建设：

- 1、应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责；
- 2、应配备一定数量的系统管理员、审计管理员和安全管理员等，应配备专职安全员，不可兼任；
- 3、应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
- 4、针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；
- 5、应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
- 6、应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
- 7、应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
- 8、应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；
- 9、应定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
- 10、应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

4.2.3 安全管理人员

依据网络安全等级保护安全管理人员控制点要求，同时结合网络安全等级保护安全设计技术要求对等级保护对象安全管理人员进行设计，内容包括人员录用、人员离岗、安全意识教育和培训，外部人员访问管理四个方面。

需制定人员录用，离岗、考核、培训规定并严格执行；规定外部人员访问流程，并严格执行。

需要有专人或小组负责人员录用，需要对专业技能、身份、背景、专业资格资质进行审核，并确定保密协议和岗位责任协议，并对被录用人员所具有的技术技能进行考核。

人员离岗及时终止各种权限，回收各类访问权限、软硬件设备，履行离职手续，并签订离职保密协定。

针对不同岗位制定不同培训计划，对安全意识、安全基础知识、岗位操作规程等进行培训，并定期对不同岗位的人员进行技能考核，要有惩戒措施。

制定外部人员访问审批流程，访问网络申请流程，访问结束立刻终止权限。高危系统访问需签订保密协议。

具体安全管理人员参考以下内容建设：

- 1、指定或授权专门的部门或人员负责人员录用；
- 2、应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
- 3、应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议；
- 4、应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
- 5、应办理严格的调离手续，并承诺调离后的保密义务后方可离开；
- 6、应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
- 7、应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；定期对不同岗位的人员进行技能考核。
- 8、应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
- 9、应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
- 10、外部人员离场后应及时清除其所有的访问权限；
- 11、获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

4.2.4 安全建设管理

依据网络安全等级保护安全建设管理控制点要求，同时结合网络安全等级保护安全设计技术

要求，对等级保护对象安全建设管理进行设计，内容包括定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评，服务供应商选择十个方面。

制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级评测、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

安全建设管理应贯穿到信息系统整个生命周期，在系统审批、建设、安全定级与备案、安全方案设计、软件开发与实施、验收与测试、系统交付与等级测评，以及服务商选择等过程均需要进行安全管理。

根据系统定级等级设计安全方案，并组织专家进行评审，经过批准后方可实施。

需要根据网络的安全保护等级和安全需求，采购使用符合国家法律法规和有关标准要求的网络产品。

对于软件开发，要确保将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；制定代码编写安全规范并要求开发人员参照规范编写代码；应具备软件设计的相关文档和使用指南，并对文档使用进行控制；应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；应保证开发人为专职人员，开发人员的开发活动受到控制、监视和审查。当软件开发采取外包模式时，还需要开发单位提供软件设计文档、使用指南及软件源代码，并对软件中可能存在的后门和隐蔽信道进行技术审查。

在项目实施过程中要指定或授权专门的小组或人员负责工程实施过程的管理，制定安全工程实施方案，并通过第三方工程监理控制项目的实施过程。

在项目测试验收阶段，应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；系统上线前还需要进行安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

系统交付使用时，应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，并对负责运行维护的技术人员进行相应的技能培训，还要提供建设过程文档和运行维护文档。

具体安全建设管理参考以下内容建设：

- 1、应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
- 2、应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
- 3、应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；

4、应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；

- 5、应确保网络安全产品采购和使用符合国家的有关规定；
- 6、应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
- 7、应在软件交付前检测其中可能存在的恶意代码；应保证开发单位提供软件设计文档和使用指南；
- 8、应指定或授权专门的部门或人员负责工程实施过程的管理；应制定安全工程实施方案控制工程实施过程；应通过第三方工程监理控制项目实施过程；
- 9、应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；
- 10、应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，应对负责运行维护的技术人员进行相应的技能培训；应提供建设过程文档和运行维护文档；
- 11、应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
- 12、应确保服务供应商的选择符合国家的有关规定，与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
- 13、应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

4.2.5 安全运维管理

依据网络安全等级保护安全运维管理控制点要求，同时结合网络安全等级保护安全设计技术要求，对等级保护对象安全运维管理进行设计，内容包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理，外包运维管理十四个方面。

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

具体安全运维管控参考以下内容建设：

1. 环境管理

在机房环境管理中需要对机房供配电、空调、温湿度控制、消防等设施指定专人或小组定期进行维护管理。

同时还应在现有的机房安全管理制度基础上继续优化，对机房人员出入、物品带进带出和机房环境安全等方面作出规定；不在重要区域接待来访人员，不将含有敏感信息的纸档文件和移动介质随意放置。

2. 资产管理

针对资产管理，应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任小组，规范资产管理和使用的行为；编制并保存与保护对象相关的资产清单。

同时应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管

理措施，确定信息分类与标识的原则和方法，对信息的使用、传输和存储作出规定。

3. 介质管理

优化介质安全管理制度，对介质存放环境、使用、维护和销毁等方面作出规定；如介质的归档和查询须有记录，并对存档介质的目录清单定期盘点。除此之外，还应对存储介质的数据安全进行管理和防范，具体如下：

- 对于需要送出维修或销毁的介质，应采用多次读写覆盖，清除介质中的敏感或重要数据，防止数据泄露；

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

- 根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行专人管理；

- 对介质物理运输过程中人员选择、打包、交付等情况进行控制；

- 保密性较高的信息存储介质未经批准不得自行销毁，销毁时必须做到双人监销，销毁记录应妥善保存；

- 重要数据存储介质带出工作环境应采取加密方式，并进行监控管理；

- 对存放的介质定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失。

4. 设备维护管理

- 对信息系统相关的各种设备、线路等指定专人或专门小组定期进行维护管理；

- 对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立申报、审批管理规定；

- 对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

- 按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器、网络设备等重要设备或系统的日志文件检查和监控；

- 建立软硬件设备维护管理制度，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等。

5. 漏洞和风险管理

针对漏洞和风险管理，需要通过漏洞扫描系统对发现的系统安全漏洞进行及时修补；需要定期安装最新补丁程序，对重要漏洞进行及时修补；定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

6. 网络和系统安全管理

- 指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析处理工作；

- 对网络设备和系统的安全策略维护、配置文件更改进行流程审批；

- 通过身份鉴别、访问控制等措施限制远程管理账户的操作行为；

- 指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

- 对能够使用系统工具的人员及数量进行限制和控制；
- 根据业务需求和系统安全确定系统的访问控制策略、文件及服务的访问权限；
- 对系统账户进行分类管理，权限设定应当遵循最小授权要求；
- 对于账户安全管理的执行情况进行检查和监督，定期审计和分析用户账户的使用情况；
- 定期检查违反规定无线上网及其他违反网络安全策略的行为。

7. 恶意代码防范管理

- 提高全体员工的网络病毒、恶意代码安全防范意识，及时升级防病毒软件；
- 在读取移动存储设备上的数据以及接收文件或邮件之前，先进行病毒检查。
- 对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定；
- 定期检查恶意代码库的升级情况并进行记录，对防病毒软件、防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，形成书面报表和总结汇报。

8. 配置管理

建立对包括网络拓扑结构、设备和系统安装的服务组件、组件版本和补丁信息、设备或系统的配置参数等进行记录和保存的管理模式；建立配置信息变更流程，及时更新配置信息库。

9. 密码管理

密码管理环节应遵循密码相关国家标准和行业标准；应使用国家密码管理主管部门认证核准的密码技术和产品，保证密码算法使用符合国家密码管理规定。

10. 变更管理

- 建立变更管理制度，重要系统变更前需经过申请审批，变更和变更方案经过评审、审批后方可实施变更；
- 应建立变更控制的申报和审批程序，如变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；
- 应明确变更过程控制方法和人员职责，必要时恢复过程应经过演练。

11. 备份与恢复管理

- 识别需要定期备份的重要业务信息、系统数据及软件系统等；
- 规定备份信息的备份方式（如增量备份或全备份等）、备份频率（如每日或每周等）、存储介质、保存期等；
- 根据数据的重要性和对系统运行的影响程度，制定数据备份和恢复策略；备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和离站运输的方法；
- 指定相应的负责人定期维护和检查备份及冗余设备的运行状况，确保需要接入系统时能够正常运行；
- 建立数据备份和恢复过程控制程序，如备份过程应记录，所有文件和记录应妥善保存；
- 建立备份及冗余设备的安装、配置、启动、操作及维护过程控制的程序，如记录设备运行过程状况，所有文件和记录应妥善保存；

- 定期执行恢复程序，检查和测试备份介质的有效性，确保可在规定的时间内完成备份恢复。

12. 安全事件处置

- 制定安全事件报告和处置管理制度，及时向安全管理小组报告所发现的安全弱点和可疑事件，如规定安全事件的现场处理、事件报告和恢复的管理职责；

- 了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，如可能来自攻击、错误、故障、事故或灾难；

- 根据安全事件在本系统产生的影响，将安全事件进行等级划分，不同安全事件采取不同的处理程序和报告程序；

- 制定的安全事件报告和响应处理程序，如规定安全事件的现场处理、事件报告和后期恢复的管理职能等；

- 在安全事件响应处理过程中，应分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

- 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

13. 应急预案管理

- 在统一应急预案框架下制定不同事件的应急预案。应急预案框架应包括启动应急预案条件、应急处理流程、系统恢复流程，以及教育和培训等内容；

- 从人员、技术和财务等方面确保应急预案执行有足够的资源保障；

- 进行人员进行培训，以了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次；

- 应急预案须定期演练，应根据不同的应急恢复内容，确定演练周期。

14. 外包运维管理

- 与外包运维服务商签订服务协议，约定外包运维的范围和工作内容；

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

- 与外包运维服务商签订的协议中应明确所有安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对基础设施中断服务的应急保障要求等。

4.3 安全运营体系

通过流程化、规范的手段，有序开展安全工作，构建持续安全运营能力，保障业务系统的安全稳定运行，制定一整套的安全服务保障体系。

由专业的安全服务人员为业务系统提供安全事件的应急响应服务，一旦发生安全问题，信息系统管理员能够在最短的时间内通知到安全专家并及时进行问题的解决，以尽可能缩小安全事件的影响范围和程度，并尽快恢复信息系统的正常运行。

提供专门的安全服务团队进行安全培训等安全专项服务，通过这些安全人员的参与，形成有效的安全运营防护体系。

4.3.1 漏洞扫描服务

漏洞扫描服务是服务人员使安全评估工具对评估目标范围内对象进行漏洞扫描，并人工验证所发现的 Web 应用漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露及配置不当等脆弱性问题。

工作方式：现场服务或远程服务。

交付物：《漏洞扫描报告》。

4.3.2 整改指导服务

提供 1 次现场整改指导服务，协助客户解读报告内容、制定整改计划、解决整改过程中的技术难题；提供 1 年免费远程技术咨询服务（含安全漏洞咨询、合规要求解读、防护策略优化建议）。

工作方式：现场服务

4.3.3 协助加固服务

在安全评估工作结束后，可以根据安全评估的结果对服务目标进行协助加固。帮助客户单位解决安全问题，降低安全风险，提高服务目标系统安全程度。

加固的方式包含人工安全加固和优化、设备安全加固建议等。

工作方式：远程服务或现场服务。

交付物：《安全加固报告》。

4.3.4 合规培训服务

开展 1 次电力系统网络安全等保合规培训（线上），覆盖客户 IT 运维人员、安全管理人员，培训内容包括等保 2.0 标准核心要求、电力行业安全防护要点、常见风险防控措施等，培训时长不少于 2 小时。

工作方式：客户提供授课场地。

交付物：课程相关资料。

4.3.5 应急支持服务

应急响应服务将根据安全风险评估的结果制定响应网络安全应急响应预案，在重大安全事件、

安全检查和其对等级保护对象系统网络安全造成严重威胁等情况下，提供及时有效的应急响应服务。

应急响应服务相当于客户给自己买了一份保险，当安全事件发生时，可以由专业的服务团队协助其分析判断事件因果、降低损失、提供有效的问题解决建议。

高级服务人员根据事件类别，通过远程和现场支持的方式协助客户对遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件信息收集、事件分析、分析报告提交、问题解决建议等。

工作方式：远程服务或现场服务。

交付物：《应急支持分析报告》。

5 方案设计清单

5.1 设备清单

序号	产品名称	参数要求	数量
1	防火墙	1. 标准 1U 机架式,国产化芯片和国产化操作系统,内存 $\geq 8\text{G}$,硬盘容量 $\geq \text{SSD } 500\text{G}$,电源: 1+1 冗余电源 网络接口: 千兆电口管理口 ≥ 2 个、千兆业务电口 ≥ 8 个、千兆业务光口 ≥ 4 个, 推荐带宽 $\geq 300\text{Mbps}$, 整机吞吐 $\geq 6\text{Gbps}$, 最大并发数 ≥ 200 万,最大新建数 ≥ 5 万/秒; 2. 支持路由模式、交换模式、旁路模式、虚拟网线工作模式、混合模式; 部署模式切换无需重启设备; 3. 支持 IPv4/IPv6 双栈协议的源地址转换、目的地址转换、双向 NAT、NAT64 等地址转换; 4. 支持静态路由、动态路由、ISP 路由; 支持基于入接口、源地址、目的地址、服务、应用的策略路由; 5. 系统预定义超过 11000 条主流攻击规则, 包含对应 IPS 规则的名称、级别、防护对象、操作系统、CVE 编号等详细信息; (提供带有 CNAS 标识的第三方权威机构检测报告并加盖制造商公章) 6. 支持检测 C&C、勒索软件、僵尸网络、挖矿软件、矿池地址等安全攻击类型; (提供带有 CNAS 标识的第三方权威机构检测报告并加盖制造商公章) 7. 支持基于源 IP 地址、目的 IP 地址、端口、协议的黑名单配置, 支持自定义黑名单生效时间; 8. 支持基于控制策略、策略路由、源 NAT 等策略的策略分析; (提供带有 CNAS 标识的第三方权威机构检测报告并加盖制造商公章)	1 台

		9. 支持一体化安全策略：可基于安全域、MAC 地址、IP 地址、服务、时间、用户、应用等属性，配置防病毒、入侵防御、内容过滤、URL 过滤、文件过滤、Web 防护、SSL 解密、弱密码防护、防暴力破解、会话老化时间等高级访问控制功能； 10. 产品制造商需具备国家信息安全测评信息安全服务资质证书；（安全工程类三级）（提供证书复印件并加盖制造商公章） 11. 产品需具备中国网络安全审查认证和市场监管大数据中心颁发的网络关键设备和网络安全专用产品安全认证证书；（提供证书复印件并加盖制造商公章） 12. 产品具备商用密码检测中心颁发的商用密码产品认证证书，且满足 GM/T 0023、GM/T 0025、GM/T 0028 要求；（提供证书复印件并加盖制造商公章） 13. 供货设备满足二级等保要求； 14. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
2	堡垒机	1. 1U 机架式，国产化芯片和国产化操作系统，内存≥8GB，数据硬盘≥2TB；千兆电口≥8 个，千兆光口≥4 光，授权资产数≥50 个，并发字符连接最大数≥50 个，并发图形连接最大数≥10 个； 2. 支持用户账号状态统计，包含用户账号上次登录时间、用户状态、过期时间等； 3. 支持目录模式对主机进行管理，可以按主机组、部门、主机网络、操作系统 4 种视图进行目录排列； 4. 支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系； 5. 支持 DB2、Oracle、MySQL、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBase8s 的协议运维代理，可实现自动登录，自动登录可直接调用本地 windows 系统的数据库客户端工具； 6. 支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能，且自动改密不借助于 Agent，无需开放 445、135、139 等高危端口； 7. 支持对常见数据库及国产数据库的自动改密功能，包括 DB2、oracle、mysql、sqlserver、PG、人大金仓、GBase8a、GBase8s、达梦数据库等； 8. 支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后方可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令； 9. 具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。动作流会按设定好的顺序进行执行，对于常见的运维工作，如升级、巡检等，均可通过此能力快速执行； 10. 产品制造商需具备国家信息安全测评信息安全服务资质证书（安全工程类三级）（提供证书复印件并加盖制造商公章）； 11. 产品具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证	1 台

		书》（提供证书复印件并加盖制造商公章）； 12. 供货设备满足二级等保要求； 13. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
3	数据库审计	1. 1U 机架式；国产化芯片和国产化操作系统，内存$\geq 8\text{GB} \times 1$；硬盘$\geq 2\text{TB} \times 1$；管理网口：千兆电口≥ 2（管理口$\times 1$，HA 口$\times 1$）；工作网口：千兆电口≥ 6、千兆光口≥ 4；SQL 每秒≥ 3000 条，吞吐量$\geq 300\text{Mbps}$/无限实例：，双向审计数据库流量$\geq 25\text{Mbps}$，峰值 SQL 事务处理数≥ 3000 条/秒，最大吞吐量$\geq 300\text{Mbps}$； 2. 审计信息能够记录执行时长、影响行数、执行结果描述、返回结果集；（提供公安部安全与警用电子产品质量检测中心颁发的检测报告并加盖制造商公章） 3. 支持 Oracle、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ 等主流数据库的审计； 4. 支持 GaussDB、Teradata、人大金仓（Kingbase）、达梦（DM）、南大通用数据库（Gbase）、Oscar、K-DB 等国产数据库的审计； 5. 支持 MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、HANA、ArangoDB、Neo4j、OrientDB 等非关系型数据库的审计； 6. 内置安全特征库不少于 900 条，如 SQL 注入、缓冲区溢出等； 7. 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单； 8. 产品具有内置规则，规则类型有 SQL 注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警；（提供公安部安全与警用电子产品质量检测中心颁发的检测报告并加盖制造商公章） 9. 设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源 IP、目的 IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想； 10. 产品应具备中国信息安全测评中心所颁发的《国家信息安全漏洞库兼容性资质证书》；（提供证书复印件并加盖制造商公章） 11. 产品制造商需具备国家信息安全测评信息安全服务资质证书（安全工程类三级）；（提供证书复印件并加盖制造商公章） 12. 供货设备满足二级等保要求； 13. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	1 台
4	终端安全及防病毒系统	1. 包含一套控制中心，配置≥ 50 个 PC 端授权，配置≥ 10 个服务器授权，； 2. 支持可视化态势大屏展示，包括终端安全管控大屏和安全概况大屏，安全概况展示内容包括防护概况、检测概况、入侵检测概况、防护风险趋势、安全动态；终端管控包括终端状态、分组分类、版本状态、安装量、防护率、在线率等； 3. 支持对 CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对	1 套

		CPU、内存达到一定阈值时客户端自动进行熔断； 4. 支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项、Web 框架、Web 服务、数据库、Web 应用、系统安装包、JAR 包、计划任务、环境变量等信息，支持从资产的维度和信息的维度去查看数据，并支持数据的导出； 5. 支持反病毒底层技术，反病毒引擎为本地反病毒引擎； 6. 提供内核级的数据防护能力，保护文件不被勒索软件或其他病毒程序恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程； 7. 提供专利级针对未知勒索病毒的诱饵防护引擎，通过自动生成的高仿真文件诱捕未知勒索病毒的攻击，并进行实时阻断； 8. 联动威胁情报，支持对 APT、木马、病毒、蠕虫、后门、勒索、挖矿、僵尸网络、漏洞利用等 10 余种不同类型的威胁进行离线鉴定； 9. 支持操作系统、数据库、中间件的等保 1 级到等保 4 级的系统基线检查，支持的操作系统、数据库、中间件类型包括 Windows、Linux、Oracle Linux、Suse、Debian、MySQL、Apache、Nginx； 10. 产品制造商需具备国家信息安全测评信息安全服务资质证书（安全工程类三级）（提供证书复印件并加盖制造商公章） 11. 为保障联动防护效果，所投终端安全及防病毒系统应与防火墙为同一品牌； 12. 供货设备满足二级等保要求； 13. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
5	EDR 管理中心服务器	1. 8 核 CPU，16G 内存，500GB 磁盘，国产芯片、CPU； 2. 供货设备满足二级等保要求； 3. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	1 台
6	服务器操作系统	1. 供货设备满足二级等保要求； 2. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	1 套
7	APT 攻击预警平台	1. 硬件规格 2U，采用国产化芯片和国产化操作系统， 标配网口：千兆业务电口≥6，千兆业务光口≥4，内存≥16G，硬盘容量≥2T，USB 口：USB 口≥2，可扩展万兆业务光口≥2，电源：冗余电源，整机吞吐量≥1.5 Gbps； 2. 支持双向流量审计，可对请求和响应内容进行审计；支持 IPv4 和 IPv6 网络环境下的部署，可同时对 IPv4 和 IPv6 网络流量分析检测； 3. 支持对 COAP、DCERPC、DHCP、DNP3、MODBUS、LDAP、FTP、SMB、IMAP、POP3 等服务识别，也支持根据实际需求自定义服务识别，根据用户配置的端口等信息自动进行服务识别； 4. 支持检测 WEB 攻击、异常访问、恶意文件攻击、可疑流量、远程控制、WEB 后门访问、DGA 域名请求、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP 欺骗、配置风险、网	1 台

		络异常、入站情报、行为分析等风险类型； 5. 支持基于 IDS 规则检测基础上通过加载 600 余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持 Primeton 插件、蚁剑插件、哥斯拉插件、冰蝎 3.0、冰蝎 4.0 等检测能力；（提供功能截图并加盖制造商公章） 6. 支持对邮件中的附件、二维码进行深度检测，防范通过附件或者二维码传播的潜在风险； 7. 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中体现； 8. 支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为； 9. 支持告警抑制功能，在重复攻击手段下能够减少相同告警数量，提高用户分析效率，可自行设置告警抑制周期、告警上限、抑制阈值、持续时间、启用维度。（提供带有 CNAS 标识的第三方权威机构检测报告并加盖制造商公章） 10. 产品制造商需具备国家信息安全测评信息安全服务资质证书；（安全工程类三级）（提供证书复印件并加盖制造商公章） 11. 供货设备满足二级等保要求； 12. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
8	入侵检测	1. 1U 软硬一体；国产化芯片和国产化操作系统，内存≥8G*1；硬盘≥2T*1；网络接口：管理口≥2 千兆电，业务口≥6 千兆电，≥4 千兆光； Console 口≥1 个；USB≥USB2.0*2； 2. 支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTP2、RADIUS、KRB5、SNMP、NETFLOW、TFTP、NNTP、COAP、GOOSE、QUIC 等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号； 3. 支持检测单台主机对多个 IP 进行扫描、单台主机对单台或多台靶机 ICMP 扫描、单台主机针对 SMB 端口向多台主机扫描、单台主机对多台靶机的 ARP 扫描等 8 种扫描行为； 4. 支持攻击链路可视化，一键溯源查看攻击全貌，将攻击者在网络中的活动路径、攻击过程以图形化方式完整地展示出来，且支持选择多条攻击链路并高亮显示，帮助用户更好理解攻击者行为； 5. 支持域名白名单、IP 白名单、URL 白名单、IDS 规则白名单、WEB 特征白名单，支持至少 5 种白名单类型； 6. 基于 IDS 规则检测基础上通过加载 600 余条深度检测特定规则插件、深度检测通用规则等进行二次深度检测，可支持 Primeton 插件、蚁剑插件、哥斯拉插件、冰蝎 3.0、冰蝎 4.0 等检测能力； 7. 支持在页面实时查看内存、交换空间、CPU、系统分区、数据分区、内存使用百	1 台

		分比、入库使用百分比等资源情况，无需登录后台，提高设备安全性； 8. 产品制造商需具备国家信息安全测评信息安全服务资质证书；（安全工程类三级）（提供证书复印件并加盖制造商公章） 9. 为保障联动防护效果，所投入入侵检测设备应与防火墙为同一品牌； 10. 供货设备满足二级等保要求； 11. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
9	恶意代码防护	1. 国产化芯片和国产化操作系统，通过部署在主机或网络边界的专用安全措施，旨在实时检测、拦截并清除病毒、木马等恶意程序，防止其破坏电网的稳定运行与数据安全。 2. 供货设备满足二级等保要求； 3. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	1 台
10	纵向加密机	1. 国产化芯片和国产化操作系统，百兆纵向加密 2. 供货设备满足二级等保要求； 3. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	2 台
11	交换机	1. 交换容量$\geq 336\text{Gbps}$，包转发率$\geq 72\text{Mpps}$； 2. 提供≥ 24个 10/100/1000BASE-T 电口，提供≥ 4个 1000 BASE-X SFP 端口； 3. 支持基于端口的 VLAN，支持基于协议的 VLAN； 4. 支持 IPv6 Ping, IPv6 Telnet, 支持 IPv6 ACL； 5. 供货设备满足二级等保要求； 6. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	2 台
12	路由器	1. 性能：交换容量$\geq 100\text{Gbps}$，转发性能：60Mpps，内存$\geq 2\text{G}$； 2. 端口：≥ 8个千兆电口，≥ 2个万兆光口； 3. 组播：静态组播，IGMPv1/v2/v3, PIM-DM, PIM-SM, PIM-SSM, PIM-SSM mapping； 4. 管理性：支持 SNMPv1/v2/v3, Telnet, SSHv1/v2 等网管协议。 5. 供货设备满足二级等保要求； 6. 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	1 台
13	反向隔离装置	国产化芯片和国产化操作系统， 设备厚度：标准 1U 网络接口：≥ 2个 100/1000M 接口（内网）；≥ 2个 100/1000M 接口（外网）；≥ 1个 100/1000M 双机热备接口（与通信接口复用）； 外设接口：≥ 2个终端管理接口(RS232)； 密文有效网络吞吐率$\geq 100\text{Mbit/s}$（100 条安全策略，1024 字节报文长度）； 满负荷数据包丢弃率 0%； 平均无故障时间（MTBF）> 50000 小时（100%负荷）； 返回确认报文长度 1bit；	1 台

		可采用硬件可信计算技术实现操作系统和应用程序安全可信； 具备激活功能，设备需登记实施人员、使用位置等供应链安全信息方可激活使用； 日志规范满足《电力二次系统安全告警日志格式规范》要求。 其它要求： 1) 只允许 UDP 协议的通信方式。 2) 具有应用网关的功能，实现应用数据的接收与转发。 3) 具有应用数据内容有效性检查功能。 4) 采用基于数字证书的数字签名/解签名技术。 5) 对文本文件形式的数据，通过编码转换技术实现半角字符转换为全角字符，保证进入 I / II 区的数据为纯文本数据。 6) 反向隔离设备提供基于国密算法的数字签名和采用电力专用加密算法进行数字加密的功能。 7) 反向隔离设备必须提供配套的文件传输程序，方便进行二次系统安全单向隔离改造。 8) 应满足传输内容纯文本 E 语言格式强过滤的要求。 9) 提供的有效期不小于 10 年的国密算法（SM2）证书。 为响应国家规定系统自主可控要求，反向隔离装置运行环境必须为厂家自主研发的自主可控操作系统，操作系统须通过安全等级四级或以上等级鉴定，并提供检验检测报告；操作系统需通过中国电力科学研究院有限公司的检验，并提供检测报告，且操作系统检测报告的受检单位必须与反向隔离装置的生产单位一致；所使用操作系统须通过国家网络安全专用产品合规检测，符合网络安全相关准入管理要求。 反向隔离装置需提供 3 年原厂商售后服务承诺函或原厂质量保证函。 供货设备满足二级等保要求； 供货设备及配套软件均须采用纯国产化产品，满足自主可控要求。	
14	网监 II 装置	国产化芯片和国产化操作系统， 1U 整层机箱； CPU≥4 核，内存≥4GB； 存储容量≥256GB 硬盘容量； 应满足≥8 个自适应网口，≥1 个 B 码对接接口； 应双路交直流电源独立供电； 内置等保三级操作系统安全增强组件； 应支持 RedHat5、RedHat6、Centos6、Centos5、Solaris 10、Windows7、WindowsXP、Windows2003、Windows2008 和国产操作系统采集 agent；	1 台

		采集信息吞吐量≥ 600 条/s; 支持监测对象数量≥ 200 个; 对上传事件信息的处理时间≤ 0.6s, 对远程调阅的处理时间≤ 2.5s; 支持采集信息的本地存储, 保存至少半年的采集信息; 支持上传事件信息的本地存储, 保存至少一年的上传事件信息; 本地日志审计记录条数≥ 10000 条; 通过 IRIG-B 同步, 对时精度≤ 1ms, 通过 SNTP 同步, 对时精度≤ 100ms; 在没有外部时钟源校正时, 24 小时守时误差应不超过 1s; 平均故障间隔时间 (MTBF) ≥ 30000h; 流量分析功能对小包解析速率≥ 18000pps。 网络安全监测运行环境必须为厂家自主研发的国产操作系统, 操作系统须通过安全等级四级或以上等级鉴定, 并提供检验检测报告; 操作系统需通过中国电力科学研究院有限公司的检验, 并提供检测报告, 且操作系统检测报告的受检单位必须与网络安全监测的生产单位一致; 装置应通过国网电力科学研究院试验验证中心的检验报告, 并提供鉴定材料; 网络安全监测需提供 3 年原厂商售后服务承诺函或原厂质量保证函。 1. 供货设备满足二级等保要求; 2. 供货设备及配套软件均须采用纯国产化产品, 满足自主可控要求。	
15	探针	1. 收集数据接入到网监 II 型装置 2. 供货设备满足二级等保要求; 3. 供货设备及配套软件均须采用纯国产化产品, 满足自主可控要求。	6 套
16	通信 330 以太网板	1. 通讯网络的 330 设备以太网板; 2. 满足二级等保要求设备的清单; 3. 330 以太网通信板沿用现有设备品牌供货。	2 块
17	对时装置	1. 双模 GPS 和北斗 2 路, ≥ 2 个网口 10/100M, ≥ 30 米天线; 2. 供货设备满足二级等保要求; 3. 供货设备及配套软件均须采用纯国产化产品, 满足自主可控要求。	1 套

5.2 服务清单

序号	服务项目	服务简介
1	漏洞扫描	漏洞扫描是脆弱性识别的重要手段, 能够帮助客户发现设备和系统中存在的风险点, 帮助客户分析技术措施的有效执行, 了解漏洞的危害, 通过及时修补完善, 避免对信息系统造成严重影响。

2	整改指导服务	提供 1 次现场整改指导服务，协助客户解读报告内容、制定整改计划、解决整改过程中的技术难题；提供 1 年免费远程技术咨询服务（含安全漏洞咨询、合规要求解读、防护策略优化建议）
3	协助加固	针对巡检和评估过程中存在安全脆弱点的网络架构、网络设备、操作系统、应用系统和数据库系统，根据安全加固工程师制定的安全加固方案进行现场协助安全加固，并提供安全加固建议
4	合规培训服务	开展 1 次电力系统网络安全等保合规培训（线上），覆盖客户 IT 运维人员、安全管理人员，培训内容包括等保 2.0 标准核心要求、电力行业安全防护要点、常见风险防控措施等，培训时长不少于 2 小时
5	应急支持服务	提供 1 次免费应急响应咨询服务，针对突发网络安全事件（如黑客攻击、数据泄露），协助客户制定应急处置方案，降低事件影响

第五章 报价文件格式

_____项目报价文件

报 价 人：_____（盖单位章）

法定代表人（负责人）或者其委托代理人：_____（签字）

_____ 年____月____日

目 录

- 文件一 报价函
- 文件二 授权委托书、法定代表人（负责人）身份证明
- 文件三 报价表
- 文件四 项目实施方案
- 文件五 偏差表
- 文件六 资格审查资料
- 文件七 合规承诺函
- 文件八 其他资料

文件一 报价函

_____（采购人名称）：

1. 我方已仔细研究了_____（采购项目名称）采购文件的全部内容，愿意以人民币（大写）_____元（¥_____）其中：不含税价格：人民币（大写）（¥_____）；增值税：人民币（大写）_____（¥_____）；税率：__%的总报价，按合同约定实施。

2. 我方承诺在采购文件规定的报价有效期内不修改、撤销报价文件。

3. 如我方成交：

（1）我方承诺在收到成交通知书后 30 天内与采购人签订合同。

（2）我方承诺在合同约定的期限内完成全部合同内容。

4. 我方在此声明，所递交的报价文件及有关资料内容完整、真实和准确，

5. _____（其他补充说明）。

报价人：_____（盖单位章）

法定代表人（负责人）或者其委托代理人：_____（签字）

_____年____月____日

文件二 授权委托书、法定代表人（负责人）身份证明
授权委托书

本人_____（姓名）系_____（报价人名称）的法定代表人，
现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清、
说明、补正、递交、撤回、修改_____（项目名称）项目报价文
件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：_____

代理人无转委托权。

报 价 人：_____（盖单位章）

法定代表人（负责人）：_____（签字）

身份证号码：_____

委托代理人：_____（签字）

身份证号码：_____

_____年_____月_____日

附：法定代表人身份证明

报价人名称：_____

单位性质：_____

地址：_____

成立时间：_____年_____月_____日

经营期限：_____

姓名：_____性别：_____年龄：_____职务：_____

系_____（报价人名称）的法定代表人（负责人）。

特此证明。

附：法定代表人身份证件复印件

法定代表人身份证件正反复印件粘贴处

附：委托代理人身份证复印件

委托代理人身份证件正反复印件粘贴处

报价人：_____（盖单位章）

_____年_____月_____日

文件三 报价表

1. 报价清单说明

本报价清单应与询价文件中的通用合同条款、技术标准和要求等一起阅读和理解。

2. 报价说明

- 2.1 报价人应根据服务工作范围及内容、合同条款等要求，结合报价人自身情况进行竞争性报价，但不得低于成本。
- 2.2 报价应包含提供服务的全部成本、合理利润、风险及税费等一切费用。
- 2.3 报价应为固定单价。对于报价人为完成本项目所必需却没有单独列项的费用，均应视为已包含在总报价中。

3. 其他说明

无。

4. 报价清单

序号	设备名称	推荐品牌	参数(参数中的所有要求需全部满足)	数量	单位	报价品牌	报价参数	含税单价 (元)	含税总价 (元)
1	防火墙	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安全 防护设计方案, 5.1 设备 清单”	1	台				
2	堡垒机	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安全 防护设计方案, 5.1 设备 清单”	1	台				
3	数据库审计	华三、安恒、亚信 等同等及以上国 产品牌	详见“第四章 网络安全 防护设计方案, 5.1 设备 清单”	1	台				

4	终端安全及防病毒系统	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	套				
5	EDR 管理中心服务器	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
6	服务器操作系统	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	套				
7	APT 攻击预警平台	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
8	入侵检测	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
9	恶意代码防护	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
10	纵向加密机	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	2	台				
11	交换机	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	2	台				
12	路由器	华三、安恒、亚信等同等及以上国产品牌	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
13	反向隔离装置	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				

14	网监Ⅱ装置	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	台				
15	探针	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	6	套				
16	通信 330 以太网板	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	2	块				
17	对时装置	/	详见“第四章 网络安全防护设计方案, 5.1 设备清单”	1	套				

注：增值税专票税率为_____。

(1) 交付前的一切风险由报价人承担；

(2) 报价人的综合单价包含但不限于与本合同相关的合同物资成本、税金、损耗、运输费、保险费、包装费、装卸费、仓储费、验收检验检测费、操作培训费以及报价人委派人员的差旅费、食宿费等为完成本合同约定的所有内容的费用；

(3) 所有设备、材料必须有出厂合格证及质量证明书；

(4) 设备及材料非采购人原因损坏的，由报价人免费返厂检修或及时更换，检修费用（包括但不限于邮寄费等）由报价人承担。

(5) 其中 1-17 项包含安防设备安装调试（包括但不限于提供所需的人力、设备、物料完成二次安防设备的安装调试工作。）及网安服

务（包括但不限于设计方案中要求的漏洞扫描、整改指导服务、协助加固、合规培训服务、应急支持服务（要求详见详见“第四章 网络安全防护设计方案, 5.2 服务清单”）。报价人在提供整改指导服务时，为确保准确识别与等级保护基线配置要求的差距，应采用专业的网络安全等级保护检查工具箱作为服务工具，且服务工具需具备中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）兼容性资质证书，提供证书复印件并加盖制造商公章。报价人在提供漏洞扫描服务时，应采用专业的 web 应用漏洞扫描服务工具与数据库漏洞扫描服务工具，且服务工具需具备中国信息安全测评中心颁发的国家信息安全漏洞库（CNNVD）兼容性资质证书，提供证书复印件并加盖制造商公章。）安防设备安装调试及网安服务的价格包括在 1-17 项价格当中，不在单独计价。

文件四 项目实施方案

(内容格式自拟,包括但不限于报价人质量保证体系和对产品的质量承诺、物资检验标准、运输保障措施、安装、调试服务措施等)报价人应根据“第四章 网络安全防护设计方案”描述编写项目实施方案。

报价人: _____ (盖单位章)

法定代表人(负责人)或者其委托代理人: _____ (签字)

_____年____月____日

文件五 偏差表

表 5-1 技术偏差表

报价人可以不提交一份对本采购文件“技术规范及技术条款”的逐条注释意见，但应根据下表的格式列出对上述条款的偏差（如果有）。未在技术偏差表中列明的技术偏差，将被视为满足采购文件要求。

项目	条款编号	偏差内容	备 注

报价人：_____（盖单位章）
法定代表人（负责人）或者其委托代理人：_____（签字）
_____年____月____日

文件六 资格审查资料

(可根据实际情况选取或增加)

附件一 报价人基本情况表

附件二 项目业绩情况表

附件一 报价人基本情况表

报价人名称						
报价人组织机构代码或统一社会信用代码						
注册地址					邮政编码	
联系方式	联系人				电话	
	传真				网址	
组织结构						
法定代表人 (负责人)	姓名		技术职称		电话	
技术负责人	姓名		技术职称		电话	
成立时间			员工总人数:			
许可证及级别			其中	高级职称人员		
营业执照号				中级职称人员		
注册资金				初级职称人员		
基本账户 开户银行				技工		
基本账户账号				其他人员		
经营范围						
备注						

本表后应附企业法人营业执照等材料的扫描件。

报价人: _____ (加盖报价人公章)

法定代表人(负责人)或者其委托代理人: _____ (签字/盖章)

_____年____月____日

附件二：项目业绩情况表

委托单位 (业主)					
服务对象名称					
项目规模					
合同金额(元)					
.....					

业绩要求：2023 年 1 月 1 日至报价截止时间止（以合同签订时间为准），提供一个国产网络安全设备（芯片、操作系统均为国产，需要提供国产化相关证明）采购项目合同金额 40 万元以上的案例，案例要求提供合同关键页、发票（发票开具时间需早于本项目采购公告之日）等。

报价人：_____（加盖报价人公章）

法定代表人（负责人）或者其委托代理人：_____（签字/盖章）

_____年____月____日

文件七 合规承诺函

合规承诺函

重庆长电渝电力工程有限公司：

为与贵司建立互惠互利的良好商业合作关系，全面响应贵司合规要求，承诺人（商业合作伙伴名称）特作出以下承诺：

一、承诺人在 XXXXXX 报价过程中，严格遵守中国、业务所在国，以及依据长臂管辖原则等可以适用的法律、法规、行业管理规范、业务监管要求、条例和惯例等，包括但不限于反欺诈、反贿赂、反垄断、反不正当竞争、外汇管制、反洗钱、知识产权保护、职业健康安全、劳工保护、环境保护、数据安全、个人信息保护和国家安全等方面的任何规定。承诺人未实施且不会实施任何可能使贵司承担法律责任的行为。

二、承诺人不向贵司及员工实施任何形式的贿赂行为，即以影响另一方与贵司业务相关的行为或决定为目的，直接或间接地提供、给予、接受或要求任何有价值物或其他好处。

三、承诺人不以影响商业决策或获取不正当利益为目的，直接或间接向政府官员、其他商业主体等任何人士或相关方提供、支付、给予、要求或承诺提供、支付、给予任何形式的贿赂、回扣及特殊待遇。

四、承诺人将全面协助和配合贵司的所有商业行为符合合规要求，并维持准确的财务记录，真实准确地在财务账簿中反映其与 XXXX 有关的所有费用支出，并妥善保管相关财务凭证。

五、贵司及贵司聘请的第三方有权对承诺人遵守本承诺函的情况开展审计。承诺人同意配合贵司的合规审计，包括配合就相关事项进行解释说明、贵司或贵司聘请的第三方提供与商业事项相关的往来文件、交易记录、财务账簿及其他会计凭证等资料。若相关的财务记录不准确，或者出现拒绝提供、隐瞒或提供虚假信息，或者存在行贿受贿、虚假报销等违规行为的嫌疑时，贵司均有权单方面以书面通知形式终止该商业事项。

六、承诺人在开展与贵司相关的业务中，如果需要再次聘请次级代理商、分销商、分包商或其他商业伙伴，应尽最大努力对业务中再聘请的第三方进行合规管理。

七、承诺人所提供的任何声明、信息和业务陈述都是准确真实的。若相关信息存

在任何更新或变化，将及时书面通知贵司，并根据贵司要求提供更新后的相关材料。

八、承诺人违反以上承诺，应承担违约责任，包括但不限于赔偿贵司因此产生的全部损失。

特此承诺。

承诺人：_____（公章）

法定代表人或其委托代理人签字：

年 月 日

文件八 其他材料

采购人要求的其他文件、报价人认为需要提及的其他文件。