采购人合同编号：

报价人合同编号：

甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评技术服务合同

采购人：

报价人：

签订时间：

签订地点：

甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评技术服务合同

委托方（甲方）：甘能化（兰州新区）热电有限公司

受托方（乙方）：

根据《中华人民共和国民法典》等相关法律法规，甲乙双方本着平等、自愿、公平和诚实守信原则，就甲方委托乙方承担甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评技术服务编制事宜，经双方协商一致，签订本合同，以便共同遵守。

第一条 项目地点：兰州新区秦川园区

第二条 项目名称：甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评技术服务

第三条 测评（评估）依据及原则：

3.1 测评（评估）依据

本次测评（评估）依据下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，凡是不注日期的引用文件，其最新版本适用于本规范。

《信息安全技术 信息系统安全等级保护基本要求》GB/T 22239-2019

《信息安全技术 信息系统安全等级保护定级指南》GB/T 22240-2020

《信息安全技术 信息系统安全等级保护实施指南》GB/T 25058-2019

《信息安全技术 信息系统安全等级保护测评要求》GB/T 28448-2019

《信息安全技术 信息系统安全等级保护测评过程指南》GB/T 28449-2019

《信息安全技术 信息安全风险评估规范》GB/T 20984-2022

《电力行业网络安全等级保护基本要求》DL/T 2614-2023

《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）

《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101 号）

《电力监控系统安全防护规定》（2024 年发改委第 27 号令）

3.2 测评（评估）原则

标准性原则：乙方方案的设计与实施应依据国家等级保护和电力行业的相关标准进行；

规范性原则：乙方工作中的过程和文档，具有很好的规范性，以便于项目的

跟踪和控制；

整体性原则：项目实施的范围和内容应当整体全面，包括安全涉及的各个层面（网络、主机、应用、物理、数据、管理制度、管理机构、人员管理、系统建设、系统运维），避免由于遗漏造成评估不准；

可控性原则：实施方法和过程需要在双方认同（认可）的范围之内，项目进度要严格按照项目工作计划执行，保证甲方对于评估工作的可控性；

最小影响原则：项目实施工作应尽可能不影响系统和网络的正常运行，不能对现有网络的运行和业务的正常运行产生明显影响（包括系统性能明显下降、网络拥塞、服务中断，如无法避免出现这些情况必须详细描述说明）；

保密原则：对项目实施中产生的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害甲方利益的行为，否则甲方有权追究乙方的责任。

上述规范除本技术规范书特别规定外，乙方所提供的测评标准均应遵循公安部、能源局相关文件要求和甲方的相关文件要求，所用的标准必须是其最新版本；如果这些标准内容矛盾时，应按最高标准的条款执行或按双方商定的标准执行；如果乙方选用本技术规范书规定以外的标准时，需提交与这种替换标准相当的或优于规定标准的证明，供甲方确认。

第四条 工作内容：

本项目全部服务内容包括自服务开始至项目全部结束，包括但不限于以下内容:

1.测评（评估）内容

1.1 等级测评

乙方依据相关国家及行业等级保护技术标准对甲方已定级信息系统进行业务现状调研，通过现场测评、整体分析及风险评估工作，全面准确评估业务系统安全保护水平与等级保护相应级别之间的差距，对于发现的问题提出整改建议，最终形成电力监控系统安全防护评估报告和等级测评报告。

测评方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地查看等多种方法。

如需在等级保护测评及电力监控系统安全防护评估实施过程中采用在线测评工具的，安全测评工具软件运行可能需要的硬件平台（如笔记本电脑、PC、工

作站等）和操作系统软件等由乙方推荐，测评软件及工具必须通过国家认可机构的安全检测/认证，且经甲方确认后由乙方提供并在测评中使用。应详细描述所使用的安全测评工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求以及使用可能对系统造成的风险等。等级保护测评应有详细的实施方案和严格的操作步骤，采取的措施应是经过测试、稳定可靠的。安全测评需要的运行环境（如场地、网络环境等）由甲方提供，乙方应详细描述需要的运行环境的具体要求。

等级测评分安全技术及安全管理两大方面共十个层面的单元测评，以及在此基础上进行的系统整体测评和后续的风险分析。

1.2 单元测评

1）物理环境测评：包括位置、访问控制、防盗窃防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电磁防护等内容。

2）网络系统测评：包括网络架构、网络访问控制、网络安全审计、边界完整性检查、网络入侵防范、网络恶意代码防范、网络设备防护等内容。

3）主机与数据库测评：包括主机与数据库身份鉴别、主机与数据库访问控制、主机与数据库安全审计、主机与数据库入侵防范、主机恶意代码防范、信息资源安全、资源控制等内容。

4）应用系统测评：包括应用系统身份鉴别、应用系统访问控制、应用系统安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制等内容。

5）数据及备份恢复测评：包括数据完整性、数据保密性、备份和恢复等内容。

6）安全管理制度测评：包括管理制度、制定和发布、评标和修订等内容；

7）安全管理机构测评：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、资金保障等内容。

8）人员安全管理测评：包括人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等内容。

9）系统建设管理测评：包括系统定级、安全方案设计、产品采购、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、等级测评、

服务商选择等内容。

10）系统运维管理测评：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、应急预案管理等内容。

1.3 整体测评

整体测评是对单元测评中发现的问题进行系统整体测评分析，包括从安全控制点间、层面间、区域间和系统结构等方面进行安全测评。

2.电力监控系统安全防护评估

根据国家及电力行业监控系统安全防护评估相关标准，在电力监控系统安全等级保护测评（即以上安全技术与安全管理测评）的基础上，增加如下测评项：资产评估、威胁评估、通用应用评估、现有安全措施有效性评估、终端检测、外设检测等。

2.1 资产评估：评估对象包括网络、主机、安全防护措施、应用系统等。根据被测评单位风险评估有关技术要求，资产评估主要考虑两个方面的内容：一是信息系统中所存储、处理、传输的主要信息，二是信息系统所提供的主要服务。通过对每一类信息和服务等级的分析，最终确定信息系统的重要性级别。资产评估具体步骤包括：资产数据整理与核实、资产重要程度分析。其中，资产数据整理与核实是根据被评估单位前期提交的资料，进行资产数据的真实性的查证与确认。资产重要程度分析是根据资产承载的数据、提供的服务，判定资产重要程度的过程。

2.2 威胁评估：是对被评估单位业务系统、网络与信息系统面临的威胁进行分析的过程。威胁评估依据《电力监控系统安全防护评估规范》提供的威胁列表，以运行与管理人员访谈的方式进行。如被评估单位能够提供历史信息安全事件统计，也可作为威胁评估的补充内容。通过威胁评估，要达到明确被评估单位信息系统面临的主要威胁，以及这些威胁的等级的目的。

2.3 通用应用评估：是对信息系统中的数据库服务、Web 服务等通用应用进行的安全配置检查，达到发现通用应用安全漏洞的目的。通用应用评估也采用人工审计和漏洞扫描两种方式进行。

2.4 现有安全措施有效性评估：是对信息系统中部署的主要安全防护措施进

行的审计，达到确定这些安全措施的管理和使用情况是否存在重大漏洞和缺陷，明确现有安全措施的有效性程度的目的。现有安全措施的评估主要采用人工检查和访谈的方式进行。主要包括防火墙、防病毒系统、防病毒网关等现有安全措施。

2.5 终端检测：主要为抽查被评估单位办公终端和上网终端是否有驻留木马、蠕虫、恶意软件，是否存在自定义共享文件夹，系统补丁是否及时更新安装，关键工作文件存放是否恰当等情况。主要通过人工查看和工具检测两种方式来进行。

2.6 外设检测：主要面向带有硬盘、内存或其他存储设备和简易操作系统的网络打印机、传真机等智能设备。具体工作为判断外设是否未设置管理员口令；是否默认开放了 FTP、TELNET、SNMP、WEB 等服务，导致攻击者可以轻易控制该设备或发送大量请求而进行拒绝服务攻击。具体工作通过人工查看配合工具监测两种方式来进行。

第五条 测评（评估）进度

甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评工作时间的总体要求为：本年度 4 月至 12 月。合同签订 7 日内，乙方按照电力监控系统安全防护评估及等级保护测评的工作要求，协助甲方完成被测评系统的等保自查和电力监控系统安全防护自评估工作，并及时提交现场评估实施方案，经同意后 3 个工作日内开展项目现场实施工作。

具体进度如下：

阶段	阶段名称	时间（工作日）
第一阶段	自查自评估、基本情况调研	5
第二阶段	现场实施阶段	10
第三阶段	问题整改阶段	18
第四阶段	复测阶段	5
第五阶段	报告编制阶段	15

第六条 编制成果及要求：

本项目全部服务内容包括自服务开始至项目全部结束，包括但不限于以下内容:

1.各系统等级保护测评报告，协助甲方办理信息系统安全保护等级备案手续，并取得备案证明

2.风险评估报告

3.电力监控系统网络安全防护方案

4.电力监控系统网络拓扑图

5.电力监控系统问题整改意见报告

6.主机与网络设备安全加固意见报告

7.网安并网全套资料制作审核

8.协助甲方人员完成相关管理制度、安全事故现场处置方案、应急预案等与电力监控系统及信息安全相关的制度建立、修订。

9. 提供网安处并网工作协调服务。

第七条 工期要求：

1.乙方自合同签订之日起60个工作日内完成信息系统评估工作，提交整改方案，并完成整改、验收测评。

2.乙方自合同签订之日起90个工作日内出具符合公安部门关于信息系统安全等级保护备案要求的测评报告及其他相关文件，并积极协助和配合甲方取得公安部门的信息系统安全等级保护备案证书。

3.因乙方相关资质或出具的相关报告不能取得甲方所在地公安部门认可，而导致甲方无法取得公安部门的信息系统安全等级保护备案证书的，由乙方自行负责与公安部门协调解决，由此产生的一切费用（如重新测评等）由乙方承担。

4.售后要求

现场测评阶段完成后应进行以下议题：

①双方确认现场测评结果，对测评发现的问题进行沟通。

②双方明确整改范围，对整改建议书内容进行沟通。

③双方根据整改范围和整改计划，指导整改实施。

第八条 付款方式：

1.本合同固定总价为元(大写 :)(含税)，税率%，不含税价： 元，税额：元，包含但不限于评估费、编制报告费、差旅费、人工费、材料费、措施费、保险、利润、食宿费及税费等全部费用，结算时不因市场变化作任何调整。

2.结算与支付：

乙方按要求完成本合同规定的内容后并出具相应正式合格的评估报告(含电子版)，经甲方核对完评估报告无误后，且乙方将评估报告提供至公安系统和调度机构备案通过后，乙方开具全额增值税专用发票及收据，甲方收到发票后于30个工作日内支付乙方全额合同款。

第九条 双方责任：

为切实保障本项目的工作质量，确保测评（评估）工作达到预期目标，对甲乙双方技术工作责任约定如下：

1、甲方责任

1）负责测评（评估）过程中相关单位和部门的协调。

2）为乙方提供良好的工作场地和环境。

3）按工作要求提供相关的资料和信息。

4）准备应急措施，负责实施过程中的紧急情况的处理。

5）明确专人全程配合乙方开展现场测评（评估）。

2、乙方责任

1）按照甲方工作章程开展工作。

2）项目内容发生变更及时与甲方代表沟通。

3）依据国家和行业相关标准开展测评（评估）工作，确保测评工作质量。

4）按照协议要求提供技术服务和成果。

5）配合甲方准备应急预案，并参与实施过程中的紧急情况处理。

6）制定具体测评（评估）实施计划方案。

7）协助甲方人员完成相关管理制度、安全事故现场处置方案、应急预案等与电力监控系统及信息安全相关的制度建立、修订，并指导完成应急演练工作。

8）针对发现的问题编制解决方案并提出整改措施，以消除风险。

第十条 合同终止：

1、乙方未能在合同期限内或双方另行确定的延期时间提交合格报告的情形。

2、因乙方自身原因，事实已无法履行合同全部和部分义务的情形，除终止本合同外，还要承担给甲方造成的损失和承担相应的法律责任。

3、法律规定的其他终止合同的情形。

发生 1、2 款情形甲方有权终止合同，乙方承担给甲方造成的经济损失和承担相应的法律责任。

第十二条 争议解决：

本合同在履行过程中发生的争议，由双方协商解决。协商不成的，可向工程所在地有管辖权人民法院诉讼。

第十三条 附则：

1、本合同自双方签字盖章后生效。

2、本合同一式壹拾份，正本贰份，副本捌份，甲、乙双方各执正本壹份，副本肆份，具有相同的法律效力。

3、本合同的附件为本合同的有效组成部分，与本合同具有相同的法律效力。

4、本合同如有未尽事宜，以国家或行业规范标准为准，遇特殊情况需补充或变更本合同内容，经双方协商一致，签订补充协议，补充协议法律效力优于本合同及磋商响应文件。

附件：服务单位廉洁承诺书

（以下签署页，无正文）

委托方（甲方）:（盖章）	受托方（乙方）:（盖章）
法定代表人:（签章）	法定代表人:（签章）
或委托代理人:（签章）	或委托代理人:（签章）
联系人：	联系人：
联系电话：	联系电话：
开户银行：	开户银行：
账 号：	账 号：
地 址：	地 址：

附件一

服务单位廉洁承诺书

甘能化（兰州新区）热电有限公司：

我方参加贵单位甘肃能化兰州新区热电项目电力监控系统级信息系统等级保护测评服务事宜，现郑重承诺如下：

1.我方在实施过程中所有提交的所有资料都真实有效、准确完整，如发现提供虚假资料，造成任何法律后果，完全由我方承担。

2.我方在本次实施服务过程中，未在注册地及所属县市（州）及以上行政主管部门作出的处罚期内，无违规、违纪、违法等不良记录。

3.我方不向贵公司工作人员及利益相关人员行贿或变相给予好处；不以任何方式向贵公司工作人员施加压力。

4.我方严格遵守廉洁自律各项规定，接受并服从贵公司组织安排。

5.我方如发现贵单位人员违背工作原则、泄露秘密、私下许诺、受贿索贿、徇私舞弊、滥用职权输送利益等情形，严格依法依规按程序向贵公司及上级部门进行实名反映，不组织、不参与群访群诉泄愤等事件。

以上承诺如有违反，我方自愿承担一切法律责任，取消我方甘能化（兰州新区）热电有限公司电力监控系统安全防护评估及等级保护测评技术服务服务资格，自愿接受贵单位按照相关规定的处理，情节严重的依照国家法律法规和相关规定移交司法机关处置。

承诺单位：（公章）

法定代表人或授权委托代理人：（签字或盖章）

年　月　日

附件二：

保密协议

甲方：甘能化（兰州新区）热电有限公司

乙方：

根据甲方相关保密制度和规定，为明确双方在电力监控及信息系统等级保护测评项目中的保密责任和义务，经共同商定，制定此《保密协议》。

一、定义

保密信息：指甲方向乙方提供的，属于甲方原有的下列资料及原有在信息载体上的材料和信息。网络扑拓图、网络资源规划图及各种方案、员工、领导的姓名及电话号码、网络设备的配置、服务器部署情况等非公开的、专业的信息和数据。

二、乙方在接受保密信息后，必须承担以下义务：

1、对保密信息谨慎、妥善持有，并严格保密，没有甲方事先书面同意，不得向任何第三方披露。

2、乙方仅可为双方合作业务之必需时，经甲方同意才能将保密信息披露给其直接或间接参与合作事项的管理人员、职员、顾问和其他雇员（统称“有关人员”），但应保证该类有关人员对保密信息严格保密。

3、若具有权力的法庭或其他司法、行政、立法机构要求乙方披露保密信息，乙方应立即通知甲方此类要求。

4、若乙方或有关人员违反本协议的保密义务，乙方须承担相应责任，并赔偿甲方由此造成的损失。

三、乙方向甲方借阅相关资料必须履行签收手续，在工作完成后，应如数归还，不得泄露或外传。甲方提供的任何资料，未经甲方同意，乙方不得复制。

四、甲方为乙方办理的出入证等证件，不允许转借他人，工作结束，立即交还。乙方人员在工作期间，未经许可不得进入非工作部门，在整个工作期间，应有甲方人员或甲方指定的人员陪同，在没有甲方人员陪同的情况下不得在院内到处走动。

五、凡与工作事项无关的内容，乙方不得询问、记录。

六、未经甲方书面同意，乙方不得将其在本协议书项下的权利和义务转让给第三方。

七、服务完成后，乙方应将系统资料全部移交给甲方，不得私自留存或擅自处理。

八、乙方保密义务的期限为无限期，其保密义务不随双方合作的终止而终止。

九、乙方违反以上条款，致使甲方在单位相关考核中被扣分或罚款处理，由此造成的单位经济损失由应由乙方承担。如泄漏甲方保密事项，给甲方造成危害，甲方将依据有关法律规定，追究乙方责任。

十、本协议的各部分构成完整的保密协议，并取代双方此前任何有关本协议所述事项的理解或协议。未经双方书面同意，本协议不得变更或修改。

十一、本保密协议一式捌份，甲方执肆份，乙方执肆份，具有同等法律效力，经双方签字盖章后生效。

十二、其他。

甲方（盖章）：

法定代表人/负责人/授权代理人（签字或签章）：

日期：　　年　　月　　日

乙方（盖章）：

法定代表人/授权代理人（签字或签章）：

日期：　　年　　月　　日