江西赣能股份有限公司丰城发电厂

生产“信息系统安全等级保护”测评

技术说明

一、项目目的

根据《中华人民共和国网络安全法》《江西省信息安全等级保护（赣等保）1号文》、《关键信息基础设施安全保护条例》等文件的要求，三级信息系统每年至少进行一次等级保护测评，为明确信息安全保障重点，积极落实相关信息安全保障条件，并落实信息安全责任，建立信息安全等级保护工作长效机制，特编制此说明。

二、现场设备状况

江西赣能股份有限公司丰城发电厂现有5号机组DCS系统、6号机组DCS系统、5、6号机组辅控DCS系统、5、6号机组NCS系统、5、6号机组系统、5、6号机组SIS系统、5、6号机组调度数据网系统等7个三级信息系统，以及7号机组DCS系统、7号机组DCS系统、7、8号机组NCS系统、7、8号机组ECMS、7、8号机组SIS系统、7、8号机组调度数据网系统的6个三级信息系统。

三、项目内容及要求

3.1 项目内容

报价人依据国家信息安全等级保护领导小组下发的等级保护标准和国家能源局等电力行业要求，对采购人5号机组DCS系统、6号机组DCS系统、5、6号机组辅控DCS系统、5、6号机组NCS系统、5、6号机组系统、5、6号机组SIS系统、5、6号机组调度数据网系统等7个三级信息系统，以及7号机组DCS系统、7号机组DCS系统、7、8号机组NCS系统、7、8号机组ECMS、7、8号机组SIS系统、7、8号机组调度数据网系统的6个三级信息系统进行等级测评和安全防护风险评估，提出《等级测评报告》《安全防护风险评估报告》和《安全建设整改方案》。并对上述13个三级信息系统为核心，数据流所经区域的主要网络设备、安全设备和服务器为对象。本次安全等级测评的分为技术安全测评和管理安全测评，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理，共10个层面的安全测评。对等保测评中发现的设备配置、安全管理及制度缺失等方面的问题进行整改，并提供售后服务技术支持及上

级机构网络安防演练、网络安全检查时的技术服务支持等。上级机构网络攻防演练、网络安全检查前后的系统安全策略完善整改、网络安全防护评估报告以及网络安全培训等技术服务。

3.2 总的要求

3.2.1 本技术规范中提出了最低的有关要求，报价人可以提供满足本项目的更高标准要求。报价人的所有服务内容必须满足国家、行业有关电力监控、信息系统安全强制性标准。

3.2.2 此次项目中的每个测评信息系统，都要求给出详细的分项报价，项目实施过程中因现场条件不具备，而没有实施的分项项目，在项目决算时应将相应的分项项目费用扣除。

3.2.3 若本次测评不能达到相应等级保护要求，报价人应在向需方提交合理合规的《安全建设整改方案》，待需方完成整改后继续免费完成本次测评服务，直到被测评系统达到相应等级保护要求。

3.2.4 报价人需在项目实施前提交《三措两案》供需方审核，以保证项目实施过程不影响被测评系统的正常运行，同时适合国家和电力行业的相关法律法规的管理规定，满足上级机构的规定和要求，否则产生的损失全部由报价人负责承担。

3.2.5 报价人需协助被测评单位完成上级主管单位网络安全检查，完善网络安全管理制度、应急预案。

3.2.6 项目实施过程中，不得影响被测评系统的正常运行，应适合国家和电力行业的相关法律法规的管理规定，满足上级调度机构的规定和要求，否则产生的损失全部由报价人负责承担。

3.2.7 本项目应按照信息系统等级保护差距分析和等级测评、信息系统安全风险评估、信息系统安全等级保护建设整改方案设计、问题整改、技术服务支持五个关键过程实施。

3.3 技术要求

3.3.1 信息系统等级保护测评要求

具体要求：工作阶段、流程、内容、以及成果交付严格遵循《网络安全等级保护测评要求》（GB/T 28448-2019）和《网络安全等级保护测评过程指南》（GB/T 28449-2018）文件，根据系统等级开展相应级别的单项测评和整体测评，测评报告内容及格式严格遵照《信息安全等级保护测评报告模板（2021 年版）》。

按照《网络安全等级保护基本要求》(GB/T 22239-2019）标准、法规，结合《电力监控系统安全防护规定》（国家发展和改革委员会 2024 年第 27 号）、《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）、《电力监控系统安全防护评估规范》（国能安全〔2015〕36 号）等标准要求，从每个信息系统的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理，共 10 个层面进行测评，并参考被测单位自身信息安全管理要求，从安全控制间、层面间、区域间和系统结构间的综合分析进行整体测评。

应依据信息系统的业务应用和内外部环境，深入调研分析各信息系统资产状况和重要性程度，以及面临信息安全的威胁。

应采用验证的方式检查工控系统的组态软件、实时数据库、历史数据库、网络设备以及信息系统的应用系统、主机系统、数据库系统、网络设备、安全设备配置是否存在安全风险。

应采用技术工具和手工测试的方法对工控系统测试，前提是不影响生产及工控系统的可用性，测试原则上采取旁路镜像的方式，并通过持续性的测试来发现问题，测试点的选择将考虑针对重点工艺、重要流程的监控。并结合工业控制系统高实时性和高可靠性的特点，制定详细的模糊测试（Fuzz 测试）错误集构建算法和精确的异常定位方法，实现工业控制系统的漏洞发现

应采用专用测试工具测试和人工现场复核方式对信息机房的消防、防雷击、防水防潮、防静电、空调、UPS、电磁辐射以及防盗等基础设备实施的防护措施进行检测检验。

应通过上位机配置验证的方式对信息系统的服务器操作系统、数据库、中间件及其网络和安全设备的安全配置及设置逐项进行检测验证，以发现口令、访问控制、安全审计等措施的安全隐患。

应通过采用网络检测工具、操作系统漏洞检测工具、数据库扫描工具、WEB 应用软件分析工具等对网络、主机等进行渗透测试分析。

应采取等级测评、安全审计、风险评估等方法，逐项对照《信息系统安全等级保护基本要求》和《电力行业信息安全等级保护基本要求》的各安全要求项，评估确定系统当前安全防护现状以及与标准要求的差距，判断安全保护建设需求及其分析。

在建设整改完成后，实施等级测评复评，收集充足数据之后，对现场测评获得的数

据进行汇总分析，形成等级测评项目的最终结论，并编制最终的《信息安全等级保护等级测评报告》。

对新上的系统定级备案，获取备案证书。

工作过程文件及项目交付成果（包括但不限于）：《信息安全等级保护等级测评报告》。

交付要求：纸质版 4 份（加盖服务机构公章）及电子版。

3.3.2 安全防护评估以及相关风险评估要求

具体要求：电力监控系统安全防护评估依据按照发改委《电力监控系统安全防护规定》（国家发展和改革委员会 2024 年第 27 号）要求，按照《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相关要求，开展安全评估工作，内容包括体系结构分析、资产分析、威胁分析、脆弱性分析、已有安全措施分析和风险分析以及。同时，针对电力监控系统安全评估中发现的各种安全风险（主要针对业务通道做具体的风险评估），评估项目组将提出安全整改建议，向采购人提供安全加固整改技术咨询支持。通过闭环方式可将系统的安全状况提升到一个较高的水平，尽可能地消除或降低系统的安全风险，最终出具《安全防护评估报告》。

工作过程文件及项目交付成果（包括但不限于）：《安全防护评估报告》等。

提交要求：纸质版 2 份（加盖服务机构公章）及电子版。

3.3.3 安全整改方案设计要求

具体要求：依照《信息安全等级保护安全建设整改工作指导意见》（公信安〔2009〕1429 号），严格遵循《信息安全等级保护安全建设整改工作指南》和《国家电力行业外网安全等级保护实施指南》各项要求，在系统测评工作的基础上，对被测单位信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全整改方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全整改技术方案设计、安全整改管理体系设计、信息系统安全产品选型及技术指标建议、安全整改项目实施计划、项目预算，整改后可能存在的其他影响。出具方案后，需以此方案为基础，开展安全整改咨询和系统加固工作，最终使被测单位安全管理和技术两方面达到相应等级的保护要求。

工作过程文件及项目交付成果（包括但不限于）：《信息安全等级保护安全整改方案》以及相关风险评估的应急预案，方案可根据整改和规划内容的重要性和复杂程度编

写。

提交要求：纸质版 2 份（加盖服务机构公章）及电子版。

3.3.4 系统安全加固服务及其他的技术服务支持要求

具体要求：根据等级测评所发现的安全问题，依据《信息安全等级保护安全整改方案》，与被测单位一起对信息系统安全建设进行整改，提供系统安全加固服务，实现全面可视化解决方案，实现威胁感知、自动资产识别、虚拟机安全隔离、数据流可视化、主机内核加固、威胁情报等功能，帮助用户自定义业务系统的安全边界，从而减少风险面的暴露。

对等保测评中发现的设备配置、安全管理及制度缺失等方面的问题进行整改，售后服务技术支持及上级机构网络安防演练、网络安全检查时的技术服务支持等。

工作过程文件及项目交付成果（包括但不限于）：《系统安全加固服务报告》。

提交要求：按现场具体情况所需。

3.4 风险控制要求

3.4.1 服务过程所面临的风险

报价人充分考虑和预知信息系统安全测评中可能存在的风险，依据《安全事件管理指南》（GB/Z 20985-2007）、《信息安全事件分类分级指南》(GB/Z 20986-2007）等标准制定了安全事件应急响应措施。

在服务过程中，测评机构会接触到系统的一些比较重要的系统信息，如安全设备配置、设备数量、IP 地址情况、拓扑结构图等，根据此部分将接触到的信息，有可能出现以下风险：

（1）信息系统敏感信息泄漏：泄漏被报价人信息系统状态信息，如网络拓扑、IP 地址、业务流程、安全机制、安全隐患和有关文档信息。

（2）验证测试对运行系统可能会造成影响：在差距测评和等级测评时，需要对设备和系统进行一定的验证测试工作，部分测试内容需要上机查看一些信息，这就可能对系统的运行造成一定的影响，甚至存在误操作的可能。

（3）工具测试对运行系统可能会造成影响：在差距测评和等级测评时，会使用一些技术测试工具进行漏洞扫描测试、性能测试甚至抗渗透能力测试。测试可能会对系统的负载造成一定的影响，漏洞扫描测试和渗透测试可能对服务器的网络通信造成一定影响甚至伤害。

3.4.2 风险控制措施

（1）签署保密协议：测评双方应签署完善的、合乎法律规范的保密协议，以约束等级保护工作双方现在及将来的行为。保密协议规定了等级保护工作双方保密方面的权利与义务。等级保护工作的成果属被测系统运营、使用单位所有，测评机构对其的引用与公开应得到被测系统运营、使用单位的授权，否则被测系统运营、使用单位将按照保密协议的要求追究测评机构的法律责任。

（2）签署委托测评协议：在测评工作正式开始之前，测评方和被测系统运营、使用单位需要以委托测评协议的方式明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等。使得测评双方对测评过程中的基本问题达成共识，后续的工作以此为基础，避免以后的工作出现大的分歧。

（3）现场测评工作风险的规避：进行验证测试和工具测试时，测评机构需要与测评委托单位充分地协调，安排好测评时间，尽量避开业务高峰期，在系统资源处于空闲状态时进行，并需要被测系统运营、使用单位对整个测试过程进行监督。在进行验证测试和工具测试前，需对关键数据做好备份工作，并对可能出现的影响制定相应的处理方案。上机验证测评原则上由被测系统运营、使用单位相应的技术人员进行操作，测评人员根据情况提出需要操作的内容，并进行查看和验证，避免由于测试人员对某些专用设备不熟悉造成误操作。测试机构使用的测试工具在使用前应事先告知被测系统运营、使用单位，并详细介绍这些工具的用途以及可能对信息系统造成的影响，征得其同意。

（4）规范化的实施过程：为保证按计划、高质量地完成测评工作，应当明确测评记录和测评报告要求，明确测评过程中每一阶段需要产生的相关文档，使测评有章可循。在委托测评协议、现场测评授权书和测评方案中，需要明确双方的人员职责、测评对象、时间计划、测评内容要求等。

（5）沟通与交流：为避免测评工作中可能出现的争议，在测评开始前与测评过程中，双方需要进行积极有效地沟通与交流，及时解决测评过程中出现的问题，这对保证测评的过程质量和结果质量有重要的作用。

（6）测试前数据备份：为避免因为测评测试造成的安全风险，测评单位在制定《测评方案》和《测评作业指导书》的同时，在现场开展测评之前，将要求配合测评人的用户单位人员对系统重要数据进行备份，以免在系统执行回退操作时丢失重要数据。

（7）测评人员管控：派出质量监督管理员对工作过程中的文档、资料进行严格管

理，防止发生失窃事件。

（8）现场检测结束后，按生产单位的保密要求彻底清除相关文档和资料。

（9）与生产单位充分沟通和协商，合理选择检测时间和地点，避免检测对生产造成不良影响。

（10）检测过程中一旦出现被测系统没有响应或中断，立即停止测试，并配合被测方人员分析情况，确定原因并恢复系统运行。

3.5 其他要求

3.5.1 报价人应针对本项目建立完整的项目组织体系并保证其有效运行。报价人的项目组织机构中应包含实施本项目所必需的各类专业技术和管理人员，其中包括但不限于项目总负责人、现场项目经理以及系统设计、集成、调试、文档管理等方面的专业人员，并且项目现场经理和项目组主要成员在参加本项目实施时不应再兼职其他工作。

3.5.2 报价人的项目组织机构中应拥有一个完整的项目实施团队，项目团队全体成员均应具有良好的服务意识和正确的工作态度。报价人拟选派的项目负责人应具有丰富的实践经验、较强的项目推动与沟通管理能力。拟选派的现场项目经理应具有同类同规模项目的实施经验，具有较强的专业技术背景和丰富的项目管理经验，具有良好的沟通协调能力。

3.5.3 报价人根据本该文件的要求，结合国家及行业规范进行深化设计，若认为存在服务内容漏缺，报价人需要补齐所需要的等级保护服务内容并自主报价，并提供全面的安全服务方案。

3.5.4 报价人的测评服务人员应具备有效期内的公安部认可的等级保护测评服务人员资格认证证书。

3.5.5 报价人提供的投标报价，中标后原则上不再做任何调整。报价人所提供的服务如果达不到招标及现场实际要求，须无条件更换，所产生的费用由报价人承担。

3.5.6 本项目所有与相关系统的分界点上工作均在报价人负责的范围之内。

3.5.7 报价人在事前必须到现场进行勘查了解，详细了解本项目系统目前的布置状况和运行状况，报价人事前没有进行现场勘查了解的，视为进行了现场勘查了解。

3.5.8 报价人在服务有效期内，技术有问题、人员力量不够或不服从管理，将严重影响到采购人信息安全及设备的安全、稳定、经济运行且无法克服时，采购人有权单方面解除合同。或采购人有权另行委托施工队伍进行紧急处理，报价人应担负全部委托费用及

由此造成的损失。

3.5.9 本文件所使用的标准如遇与报价人所执行的标准发生矛盾时，按较高标准执行。

3.5.10 本文件经双方确认后作为订货合同的技术附件，与合同正文具有同等效力。

3.5.11 报价人在提供技术服务时，不能影响现有应用系统正常运行。报价人在项目实施前需给出详细的方案，对可能影响现有应用系统正常运行的操作提出可靠的解决方案或制定应急预案等防范措施并报需方审核。

3.5.12 技术服务所必须使用的软、硬件测试工具由报价人提供，但必须有相应检测机构出具的合格证书。

3.6 资质要求

报价人应满足下列要求并提供下列相关资料，包括但不限于：

3.6.1 提供工商行政管理局登记注册并经年检（审）合格的营业执照或法人证书（复印件加盖公章，并提供原件备查）。

3.6.2 具有公安部颁发的《网络安全等级测评与检测评估机构服务认证》证书（复印件加盖公章，并提供原件备查）。

3.6.3 投标测评机构的测评人员具备公安部认可的等级保护测评服务人员资格认证测评师证，且相关证书加盖公章、提供用人合同、社保证明（复印件加盖公章，并提供原件备查）。

3.6.4 具有公安部认可的 2 名及以上 DJCP 高级测评师证书，提供用人合同及社保证明（复印件加盖公章）。

3.6.4 报价人 2023 年 1 月 1 日（合同签订日期为准）至今，600MW 及以上火电机组等保测评业绩不少于 2 个（提供合同复印件，并提供原件备查）。

3.6.5 具备公安部颁发的《网防安全服务中心》或《网安防护技术服务站》证书。（复印件加盖公章，并提供原件备查）。

3.6.6 近五年（2020 年 1 月 1 日至今）未受到国家网络安全等级保护工作协调小组办公室和公安部第三研究所警告、处罚、整改（提供网上查询截图并加盖公章）。

四、供货清单（包括但不限于此）

供货清单为大致的技术服务清单列表，仅满足本项目最低要求，不承诺其完整性，报价人应保证满足采购人的合理范围内的项目需求。提供的产品必须满足现场的要求，保证技术服务的完整性和准确性。否则作退货处理，所产生的一切损失均由报价人承担。

4.1 技术服务成果

4.1.1 等级测评

依据国家信息安全等级保护领导小组下发的等级保护标准和国家能源局等电力行业要求，对系统进行等级测评，提出《等级测评报告》和《安全建设整改方案》。

4.1.2 安全防护风险评估

按照发改委《电力监控系统安全防护规定》（国家发展和改革委员会2014年第14号）要求，按照《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的要求，本着"实事求是、客观公正"的原则，对系统实施安全防护风险评估，提出《电力监控系统安全防护风险评估报告》。

4.1.3 安全整改方案设计

在系统测评工作的基础上，对被测单位信息安全管理和技术方面现状进行全面的分析，制订信息安全等级保护安全整改方案，方案内容包含但不限于：信息安全背景、政策与技术标准依据、当前风险分析、安全需求分析、总体安全策略、安全整改技术方案设计、安全整改管理体系设计、信息系统安全产品选型及技术指标建议、安全整改项目实施计划、项目预算，整改后可能存在的其他影响。

4.1.4 系统安全加固服务及其他技术服务支持

根据等级测评所发现的安全问题，依据《信息安全等级保护安全整改方案》，与被测单位一起对信息系统安全建设进行整改，提供系统安全加固服务，实现全面可视化解决方案，实现威胁感知、自动资产识别、虚拟机安全隔离、数据流可视化、主机内核加固、威胁情报等功能，帮助用户自定义业务系统的安全边界，从而减少风险面的暴露。

对等保测评中发现的设备配置、安全管理及制度缺失等方面的问题进行整改，售后服务技术支持及上级机构网络安防演练、网络安全检查时的技术服务支持等。

4.1.5 文档资料

报价人在服务工作各阶段，应形成书面项目服务成果资料文件并及时提交采购人确认。项目实施完成后，应集中提交所有项目文档，项目主要提交文档至少包括以下文件：

（1）《项目实施计划书》

（2）《信息系统等级测评方案》

（3）《信息系统安全等级测评报告》

（4）《电力监控系统安全防护风险评估报告》

（5）《信息安全等级保护安全建设整改方案》

4.2 交付进度

4.4.1 本期项目的工期为：2025 年 03 月 01 日-2025 年 11 月 30 日。全部现场测试工作任务应在相应机组的停机修理期间完成，现场实际工作不超过 60 天。本期项目的所有工作任务应在 2025 年 11 月 30 日前完成，通过验收，并满足国家公安机关及电力系统对等级保护工作的要求。如时间有变动，采购人另行通知，报价人无条件服从。

五、验收条件

报价人应坚持“科学、公正、客观、有效”的第三方测评原则，信息系统安全等级保护测评过程及测评文档应完全依照并满足《信息安全等级保护管理办法》（公通字〔2007〕43 号）、《信息系统安全等级保护基本要求》(GB/T 22239－最新版）、《信息系统安全保护等级实施指南》《信息系统安全等级保护测评要求》《信息系统安全等级保护测评过程指南》和《网上办税系统安全保障要求（试行）》、《网上办税系统信息安全测评准则（试行）》和《网上办税系统信息安全基本技术规范》等国税行业安全测评标准，实施等级保护测评。《安全建设整改方案》应根据测评结果，结合“重点保护”“适度保护”“同步建设”等原则进行设计。项目质监组将贯穿整个项目实施过程，监督各组人员现场行为和测评质量。

5.1 具体质量要求：

5.1.1 根据各信息系统的定级结果，选择和使用对应的基本安全要求，明确信息系统应该具有的安全保护能力。

5.1.2 依据《信息安全等级保护基本要求》标准分层面采取各种安全措施时，还将考虑以下总体性要求，保证信息系统的整体安全保护能力：

5.1.3 报价人在开展正式测评前需要提出基于技术规范书要求、基于等级保护测评规范的《测评方案》和《测评指导书》，方案中应详细描述测评双方的工作准备、工作过程及人员组织等情况。

5.1.4 报价人应充分考虑和预知信息系统安全测评可能存在的风险，并采取措施防范风险事件的发生，必要情况应根据《信息安全事件管理指南》(GB/Z20985 最新版）制订安全事件应急响应措施。

5.2 项目验收：

5.2.1 报价人提供的服务应满足合同及技术规范书、技术协议中约定的全部服务内容。

5.2.2 报价人提供合同及技术规范书、技术协议约定的全部服务成果。

5.2.3 报价人应提交验收流程、验收方法和验收依据并提供详细的验收测试大纲或计划，大纲中应明确规定验收项目和必须满足的要求。大纲必须经采购人确认后方可生效。

5.2.4 报价人应对所有正式交付件的综合质量审查负责，指定各交付件的相关责任人，明确相关职责。

5.2.5 采购人对报价人是否完全交付项目《信息系统安全等级测评报告》《电力监控系统安全防护评估报告》《信息安全等级保护安全建设整改方案》等资料进行验收。验收报告需双方代表签字认可。

5.3 付款条件

技术服务完成后，报价人完全交付项目《信息系统安全等级测评报告》《电力监控系统安全防护评估报告》《信息安全等级保护安全建设整改方案》等资料，完成验收手续后，各项服务验收合格后方可进行付款。

六、质量保证条款

本招标项目售后服务期为一年，售后服务内容：负责对交付成果中的文档进行免费修正、优化、补充和完善，并负责对测评范围内的安全整改和项目实施提供免费技术支持和人工服务，以及上级机构网络安防演练、网络安全检查时的免费的技术服务支持等。并提供 7*24 小时售后服务电话技术支持。

技术评分标准（生产“信息系统安全等级保护”测评）

序号	项目	内容	标准分
1	同类项目业绩	1、提供完成类似单个项目的等级测评服务项目业绩的，满足招标文件最低业绩要求得10分；满足投标文件基础上，每提供一个同类项目业绩加2分，最高得20分。 **评审依据：提供有效业绩合同复印件，其中满足招标要求（指招标公告中投标人资格标准所述业绩要求）。**	20
2	主要技术条款	1、完全符合招标文件技术条款要求得18分，每一项不满足（按最小排序子项）的扣3分，扣完为止。产品参数优于招标文件要求和配置要求的酌情加1～4分。 **评审依据：投标文件响应情况。**	22
3	企业综合技术能力	1、项目经理应具有公安部信息安全测评中心或中关村测评联盟颁发的高级信息安全等级测评师证书得2分，在此基础上，每满足以下一项加2分，本项共计6分。 1.1具有中国信息安全测评中心颁发的CISP-DSG证书（注册数据安全治理专业人员）加2分； 1.2具有中国信息安全测评中心颁发的原创漏洞证明的加2分。 **评审依据：投标人在响应文件中提供项目经理相应证书复印件及近3个月社保缴纳证明并加盖投标人公章佐证。** 2、项目技术负责人具有公安部信息安全测评中心或中关村测评联盟颁发的高级信息安全等级测评师证书得2分，在此基础上，每满足以下一项加1分，本项共计6分。 2.1具有数据安全认证专家CDSP证书的加1分； 2.2具有重要信息系统保护人员证书的加1分。 **评审依据：投标人在响应文件中提供技术负责相应证书复印件及近3个月社保缴纳证明并加盖投标人公章佐证，未提供不加分。否则不加分。** **2、项目实施团队人员能力，本项最高加18分。** 2.1、具有国家职称部门颁发的互联网技术高级工程师每提供一个得3分最高加6分。 **评审依据：提供项目组成员国家职称部门颁发的互联网技术高级工程师证书扫描件加盖公章及近3个月投标人为其缴纳的社保证明复印件并加盖投标人公章佐证，未提供不加分。** 2.2、投标人成员具备注册网络安全渗透评估专业人员NSATP-A高级证书的3分，最高加6分。 **评审依据：提供项目组成员**注册网络安全渗透评估专业人员NSATP-A高级证书**复印件并加盖投标人公章佐证及近3个月社保缴纳证明，未提供或提供无效者不得分。** 2.4、实施团队具有网络安全服务能力，能对项目实施过程提供有效的管理，投标人中级测评师具备专业的网络与信息安全管理员-互联网审核员职业技能证书的，每提供一个加2分，最多加6分。 **评审依据：提供项目组成员网络与信息安全管理员证书及技能人才评价全国联网查询截图复印件和投标人在近3个月连续为其缴纳社会保险的证明材料并加盖投标人公章佐证；否则，不予加分。**	30
5	管理组织机构及人员投入	组织机构健全，人员配置满足项目需求得4分，组织机构优于标书要求加0-1分。组织机构人员不满足招标文件要求时：项目经理、技术负责人、兼职安全员不满足或缺失本项得0分，其他人员不满足、缺失每人扣1分；扣完为止。**评审依据：投标文件响应情况。**	5
6	施工进度计划	满足招标方要求有进度图，前期设计、物资计划、施工主要节点安排合理，科学可行，计划详实，此项得4分。每缺少一项扣1分；每一项计划不详实，安排不科学合理，酌情扣0-1分；扣完为止。**评审依据：投标文件响应情况。投标方投标文件提供的网络进度图、工程进度表等资料进行评分。**	4
7	安全保证措施	安全管理体系健全、安全保障、监督措施完善，得6分。无安全管理体系、安全保障措施本项得0分，安全保障、监督措施不完善，每一项扣酌情扣1-2分。**评审依据：投标文件响应情况。**	6
8	环境、职业健康	提供环境、职业健康管理体系认证、保证措施得基本分3分；无环境、职业健康管理体系认证本项得0分。保证措施不完善酌情扣0-1分。评审依据：投标文件响应情况。	3
9	价格评分	价格得分满分为10分：价格分采用低价优先法计算，即满足磋商文件要求且最终报价最低的报价为评审基准价，其价格分为满分。其他磋商响应投标人的价格分统一按下列公式计算：报价得分=（评审基准价／磋商报价）×10%×100，计算分数时四舍五入取小数点后两位。	10
合计			100