电力监控系统安全防护评估及信息系统

安全等级保护测评项目

技术规范书

**二零二一年三月**

1. **总则**
   1. **引言**

为了落实公安部、国家能源局关于电力监控系统安全等级保护要求，进一步增强电力监控系统安全防护能力，确保电力监控系统安全稳定运行，依据《信息系统安全等级保护基本要求》（GB/T 22239-2008）、《电力行业信息系统安全等级保护基本要求》（电监信息[2012]62号）、《电力监控系统安全防护规定》（国家发展改革委员会[2014年]第14号令）、《电力行业网络与信息安全管理办法》（国能安全[2014]317号）和《电力行业信息安全等级保护管理办法》（国能安全[2014]318号）等制度和标准要求，进行本次电力监控系统等级保护测评与安全防护评估。

* 1. **适用范围**

本技术规范适用于电力监控系统等级保护测评及安全防护评估技术服务项目的采购，包括技术服务要求和验收要求。

* + 1. 本技术规范提出的是最低限度的技术要求。凡本技术规范中未规定，但在相关国家标准、电力行业标准或IEC标准中有规定的规范条文，投标方应按相应标准的条文进行服务供应说明。
    2. 如果投标方没有以书面形式对本技术规范的条文提出异议，则招标方认为投标方提供的服务完全符合本技术规范。
    3. 本技术规范所建议使用的标准如与投标方所执行的标准不一致，投标方应按更严格标准的条文执行或按双方商定的标准执行。
  1. **标准和规范**

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，除本技术规范书特别规定外，投标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招标方的相关文件要求，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；如果投标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，供招标方确认。

* 《信息安全等级保护管理办法》（公通字[2007]43号）
* 《GB/T 22239-2019信息安全技术网络安全等级保护基本要求》
* 《GB/T 28448-2019信息安全技术网络安全等级保护测评要求》
* 《GB/T 28449-2018信息安全技术网络安全等级保护测评过程指南》
* 《GB/T 20984-2007信息安全技术信息安全风险评估规范》》
* 《GB/T 37138-2018电力信息系统安全等级保护实施指南》
* 《GB/T 36324-2018 信息安全技术工业控制系统信息安全分级规范》
* 《GBT 22240-2020)信息安全技术网络安全等级保护定级指南》
* 《关于开展电力行业信息系统安全等级保护定级工作的通知》（电监信息〔2007〕34号）
* 《电力行业信息系统安全等级保护基本要求》（电监信息[2012]62号）
* 《电力行业网络与信息安全管理办法》（国能安全[2014]317号）
* 《电力行业信息安全等级保护管理办法》（国能安全[2014]318号）
* 《电力监控系统安全防护规定》（国家发展改革委员会[2014年]第14号令）
* 《电力监控系统安全防护总体方案》国能安全[2015]36号
* 《发电厂监控系统安全防护方案》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
  1. **权利和职责**

为切实保障本项目的工作质量，确保测评及评估工作达到预期目标，对招标方及项目实施方双方技术工作责任约定如下：

* + 1. **招标方责任**
* 负责测评实施过程中同相关单位和部门的协调。
* 为项目实施方提供良好的工作场地和环境。
* 按工作要求提供相关的资料和信息。
* 准备应急措施，负责实施过程中的紧急情况的处理。
  + 1. **项目实施方责任**
* 按照招标方工作章程开展工作。
* 项目内容的变更及时与招标方代表沟通。
* 按照协议要求提供技术服务和成果。
* 确保测评及评估工作质量。
* 配合招标方准备应急预案和实施过程中的紧急情况处理。
* 负责按时完成所有工作。

同时，双方都必须遵循保密要求。

* 1. **项目范围**

电力监控系统信息安全等级保护测评与安全防护评估范围如下：

（1）本次项目安全服务具体招标范围包括：对XXX系统、XXX系统，开展等级保护定级、备案、等级测评、安全防护评估、安全整改方案设计和系统安全加固服务。

（2）电力监控系统等级保护测评工作需提交主管部门及监管机关认可的等级保护测评报告，电力监控系统安全防护评估工作交付物为主管部门及监管机关认可的安全防护评估报告。等级保护测评及安全防护评估报告必须于2021年4月30日完成。

（3）根据国家等级保护相关标准，电力监控系统的安全等级保护测评共10个层面进行测评，主要包括以下内容：

安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心等五个方面的安全测评；

安全管理测评：安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等五个方面的安全测评；

电力监控系统安全防护评估的主要内容包括：资产评估、威胁评估、脆弱性评估、现有安全措施有效性评估、白客渗透检测、终端检测、外设检测等。

针对移动互联、工业控制系统提出了特殊要求，称为安全扩展要求，检查内容包括：

移动互联扩展要求：无线接入点的物理位置、边界防护、访问控制、入侵防范、移动终端管控、移动应用管控、移动应用软件采购、移动应用软件开发、配置管理。

工业控制扩展要求：室外控制设备物理防护、网络架构、通信传输、访问控制、拨号使用控制、无线使用控制、控制设备安全、产品采购和使用、外包软件开发。

|  |  |  |
| --- | --- | --- |
| 项目 | 服务内容 | 工作描述 |
| 等级测评 | 项目准备及现场调研 | 协助对信息系统物理环境、网络、终端、数据、安全管理等进行调研。 |
| XXX系统、XXX系统、XXX系统定级、备案 | 疏理信息系统定级工作，完成信息系统定级报告及定级材料的准备； 整理、补充信息系统备案所有相关的文档，完成相应信息系统等级保护备案工作，然后送到所属地市公安机关备案。 |
| 信息系统差距分析 | 对定级的信息系统，依照《GBT 22240-2020)信息安全技术网络安全等级保护定级指南》进行逐个对照，分析信息系统安全情况与等级保护基本要求的差距，完成信息系统等级保护差距分析报告。 |
| 等级保护安全整改 | 委派专业的信息安全网络评估师（能源）或主任审核员；按照《信息系统安全等级保护基本要求》协助落实相关的等级保护建设整改工作，等级保护整改实施具体内容包括安全管理制度修订、安全技术整改、形成安全配置基线、进行安全增强配置和调试工作、实施等保相关培训、安全风险管理工作落实等工作内容，提升信息系统的安全防护能力，确保信息系统满足国家等级保护相应等级要求。 |
| 等级保护测评 | 参照《GBT 22239-2019 信息安全技术 网络安全等级保护基本要求》和《GB T 28448-2019 信息安全技术 网络安全等级保护测评要求》等标准规范要求，对信息系统开展信息系统等级保护测评工作。 |
| 输出《信息系统等级保护测评报告》 | 服务目标为通过公安部门的等级保护检查，输出《信息系统等级保护测评报告》 协助用户取得公安机关备案证明。 |
| 电力监控系统、XXX系统、网络安全监测装置接入业务系统安全防护评估 | 编制防护评估方案 | 依据《电力监控系统安全防护总体方案》（国能安全[2015]36号配套文件） 编制方案评估方案。 |
| 安全防护评估 | 安全防护评估范围  一是技术安全评估，二是管理安全评估。其中技术安全评估主要包括物理安全、网络安全、主机安全、应用安全和数据安全等五个层面，管理安全评估包括安全管理机构、管理制度、人员安全、系统建设管理和系统运维管理。  本次安全评估工作包括体系结构分析、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。 |
| 出具防护评估报告 | 依据《电力监控系统安全防护评估规范》 （国能安全[2015]36号配套文件） ，编制防护评估规范。 |

1. **技术规范**
   1. **测评及评估原则**

本项目实施方案设计与具体实施应满足以下原则：

* + 1. 保密性原则：项目实施方应与招标方签订保密协议，对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害招标方的权益，否则招标方有权追究投标方的责任。
    2. 标准性原则：测评及评估方案的设计与实施应依据国家的相关标准进行。
    3. 规范性原则：项目实施方工作中的过程和文档，应具有规范性，便于项目跟踪和控制。
    4. 可控性原则：项目的进度应符合进度安排，保证招标方对测评工作的可控性。
    5. 整体性原则：测评及评估的范围和内容应系统、全面、规范，满足等级保护和安全防护评估的相关基本要求。
    6. 最小影响原则：技术测评及评估工作应尽可能小的影响在线系统和网络的正常运行，不能对现有运行系统造成影响。在线测评及评估应在招标方许可的条件下进行。
  1. **实施要求**

投标方应详细描述电力监控系统等级保护测评及安全防护评估的整体实施方案，包括项目概述、等保测评方案、安全防护评估方案、项目实施方案、时间安排、阶段性文档提交和验收标准等。投标方应详细描述测评及评估人员的组成、资质及各自职责的划分。投标方应配置经验丰富的测评及评估人员进行电力监控系统等级保护测评及安全防护评估工作。

* + 1. **测评及评估方法**

测评及评估方法包括访谈、检查和测试三种方法，可细化为文档审查、配置检查、工具测试和实地察看等多种方法。

如需在电力监控系统等级保护测评及安全防护评估实施过程中采用在线测评工具，各种工具软件由项目实施方推荐，经招标方确认后由项目实施方提供并在工作中使用。

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项目实施方推荐，经确认后由项目实施方提供并在测评中使用。安全测评需要的运行环境（如场地、网络环境等）由招标方提供，项目实施方应详细描述需要的运行环境的具体要求。

* + 1. **工作进度**
       1. 筹划准备阶段

工作周期：1周

工作内容：对被测评及评估系统防护现状进行详细分析和调研，初步确定测评及评估实施方案、范围，收集材料，签署保密协议，组建测评及评估项目组，并进行进场实施前的安全教育工作，同时完成检测工具、装备配置等各项准备工作。

* + - 1. 启动阶段

工作周期：1～2个工作日

工作内容：项目组进驻被测单位，收集分析信息资产资料、网络资料、业务系统资料和信息安全管理制度方针等相关测评所需材料，并召开启动会，就测评及评估工作具体事宜进行落实，包括确定测评及评估计划安排、测评及评估范围、测评及评估内容和配合需求等。

* + - 1. 现场测评

工作周期：4-5个工作日

工作内容：项目组从管理和技术两个方面入手，开展被测单位测评及评估工作，包括安全区划分、网络专用，评估管理和制度、基础网络、业务系统、通用服务、主机系统、数据库系统、现有安全措施等。

测评及评估方法有顾问访谈、日志审计、人工查看、漏洞扫描、自动化工具采集、白客渗透等。

现场工作结束后，测评及评估工作小组对现场测评情况进行初步整理汇总，向被测单位领导和系统管理员等汇报现场阶段工作情况。

* + - 1. 结论分析报告编制阶段

工作周期：1周

工作内容：项目组对检测情况和采集的数据进行分类统计、风险计算、综合分析与评估，撰写《等级保护测评报告》、《电力监控系统安全防护评估报告》及《系统安全加固服务报告》。

* + - 1. 整改技术支持阶段

工作周期：根据整改进度而定

工作内容：项目组针对现场测评及评估发现的问题，出具整改建议后，向被测单位提供整改技术咨询支持。

* + 1. **风险控制**

测评及评估工作本身也会引入安全风险，必须加强测评及评估过程中的风险控制。项目实施前，双方应充分讨论并明确测评及评估对系统可能带来的风险和隐患，确定测评及评估对象、测评及评估方法和工具，并制定应急恢复措施。

（1）操作的申请和监护

测评及评估操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

（2）人员与数据管理

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备（系统）或临时搭建的模拟环境进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统在线应急处置能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评。

* 1. **等级保护测评内容**

根据国家等级保护相关标准，本次项目的安全等级保护测评应包括以下内容：

**2.3.1 安全物理环境**

物理安全测评是对信息系统的机房和办公场所的物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护等方面的安全状况。

**2.3.2 安全通信网络**

网络安全测评是对信息系统的网络系统安全防护情况进行测评，包括网络结构安全、通信传输、可信验证等方面的安全状况。

**2.3.3 安全区域边界**

安全区域边界是对信息系统的边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全状况。

**2.3.4 安全计算环境**

安全计算环境是对信息系统的身份鉴别、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、个人信息保护等方面的安全状况。

**2.3.5 安全管理中心**

安全管理中心是对信息系统的系统管理、审计管理、安全管理、集中管控进行测评。

**2.3.6 安全管理制度**

安全管理制度测评将通过访谈和检查的形式评测安全管理制度的制定、发布、评审和修订等情况。主要涉及安全主管人员、安全管理人员、各类其它人员、各类管理制度、各类操作规程文件等对象。

**2.3.7 安全管理机构**

安全管理机构测评将通过访谈和检查的形式评测安全管理机构的组成情况和机构工作组织情况。主要涉及安全主管人员、安全管理人员、相关的文件资料和工作记录等对象。

**2.3.8 安全管理人员**

安全管理人员测评将通过访谈和检查的形式评测机构人员安全控制方面的情况。主要涉及安全主管人员、人事管理人员、相关管理制度、相关工作记录等对象。

**2.3.9 系统建设管理**

系统建设管理测评将通过访谈和检查的形式评测系统建设管理过程中的安全控制情况。主要涉及安全主管人员、系统建设负责人、各类管理制度、操作规程文件、执行过程记录等对象。

**2.3.10 系统运维管理**

系统运维管理测评是对信息系统运行维护过程中的环境管理、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、外包运维管理等情况进行测评。

* 1. **安全防护评估内容**

根据电力监控系统安全防护评估相关标准，在系统等级保护测评的基础上，增加如下评估项：资产评估、威胁评估、通用应用评估、基础设施安全评估、体系结构安全评估、系统本体安全评估、全面安全管理评估、安全应急能力评估、现有安全措施有效性评估等。

* + 1. **资产评估**

资产评估对象包括：网络、主机、安全防护措施、应用系统等。根据安全防护评估有关技术要求，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。

* + 1. **威胁评估**

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。

* + 1. **通用应用评估**

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。

* + 1. **基础设施安全评估**

基础设施评估是对电力监控系统所处机房的物理安全防护情况，包括防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施实施情况，电子门禁的使用情况等进行评估。

电力监控系统设备及线缆的部署情况，包括服务器、网络设备、安全设备的安装情况，通信线缆和电源线的铺设情况，设备电力供应情况等

* + 1. **体系结构安全评估**

体系结构评估应重点检查16字方针“安全分区、网络专用、横向隔离、纵向认证”的落实情况，重点针对网络边界防护措施、横向隔离、纵向认证等关键防护措施的执行情况，安全接入区的设置情况、无线网络防护等。

* + 1. **系统本体安全评估**

系统本体安全评估是对电力监控系统自身安全防护情况，包括软、硬件使用和策略配置等进行评估：

1. 移动存储介质使用情况，包括硬盘、U盘或其它存储设备；
2. 操作系统、网络设备、应用系统用户口令使用情况；
3. 操作系统、网络设备、应用系统用户权限分配情况；
4. 主机、交换机、路由器等设备、应用系统的安全策略配置及加固情况，尤其是Windows系统、非国产网络及安全设备。
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。
6. 外设检测：主要检测带有硬盘、内存或其它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。
   * 1. **全面安全管理评估**

全面安全管理评估是从管理角度对单位电力监控系统概况进行评估，重点检查安全防护规定落实情况；

制度建立及主管领导、管理机构和工作人员履职情况，信息安全责任制落实情况；

运维人员的安全管控情况；

电力监控系统安全防护评估工作开展情况；

信息安全宣传教育、领导干部及各级人员网络与信息安全基础培训、信息安全人员专业技术培训情况等。

* + 1. **安全应急能力评估**

安全应急能力评估是对系统的安全有效性、业务的连续性和备用、灾备能力进行评估。

备用与容灾能力的建设情况，包括系统的冗余设备部署情况，设备配置的备份情况等；

网络与信息安全应急预案的制定、修订情况，包括应急预案是否健全，是否具有针对性和可操作性等；

应急技术支撑队伍建设、应急演练的执行情况；

重大网络安全事件处置情况。

* + 1. **现有安全措施有效性评估**

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、入侵检测/防御装置、防病毒网关、单向隔离装置、纵向认证装置等现有安全措施。

* + 1. **白客渗透检测**

白客渗透检测包括两个方面的内容：外部渗透和内部渗透。

外部渗透主要是检测被评估单位面对来自互联网恶意入侵者渗透的防御能力。主要范围为被评估单位对互联网发布节点的应用服务器、对外网站服务器及下属网站服务器等，模拟黑客进行渗透性测试。

内部渗透主要是检测被评估单位面对来自内部恶意破坏者渗透或窃密的防御能力。主要范围为被评估单位内网门户、内部网站等；因电力监控系统影响面广，在对生产区系统进行渗透检测时应签订保密协议；若出现紧急情况；现场应急处理人员所属单位应是国家互联网应急中心(CNCERT)“省级及以上支撑单位。

* + 1. **终端检测**

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。

* + 1. **外设检测**

外设检测主要面向带有硬盘、内存或其它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。

* 1. **测评及评估流程**

根据国家等级保护相关标准，电力监控系统安全等级保护测评流程分为四个阶段：测评准备阶段、方案编制阶段、现场测评阶段、分析与报告编制阶段。测评完成后，提供整改建议书，配合招标方根据测评范围进行整改实施。

电力监控系统的安全等级保护测评流程如下图所示：



电力监控系统安全防护评估工作基本流程将依照《电力监控系统安全防护评估规范》进行，分前期交流和启动准备阶段、现场数据采集和评估阶段、风险计算和分析阶段，以及总结阶段。



* 1. **配合招标方完成电厂安全分区和边界防护自查整改。包括但不限于以下几点：**

(1)检查整改生产控制大区网络违规外联、远程运维等问题；

(2)检查正反向隔离装置、Ⅰ/Ⅱ区防火墙正确配置安全策略，应符合安全防护原则；

(3)检查服务器、工作站等主机存在安全漏洞以及远程登录风向，禁用不必要的服务和端口，同时进行系统加固工作；

(4)操作员工作站和运维工作站等禁止移动介质和无线公网的使用。

(5)配合招标方建立健全责任体系。

(6)配合招标方提高网络安全应急处置能力。

(7)配合招标方加强人员管理和培训。

(8)投标方根据本招标文件的要求，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，投标方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。

1. **项目服务商要求**
   1. **对投标方的要求**

3.1.1投标方要求

投标方应仔细阅读本技术规范书所列的各项规范，所提供的安全服务应满足本技术规范书提出的要求。投标方也可以推荐满足本技术规范的其他方案，但必须对其在技术规范方面与本技术规范书之间所存在的差异加以详细说明。若无说明，则按对投标方不利的方面理解。

投标方应为具有法人资格且根据商业法规经营的国内企业实体且应是公安部推荐测评机构名录内；具备承担本次招标的资质条件、能力和信誉。

投标方单位需符合《中华人民共和国政府采购法》第二章第22条规定；即供应商必须是近五年没有被主管部门被停业整顿且处于停业期、投标资格被取消或者财产被接管、冻结和破产状态；是在境内依法注册的独立法人或组织。

投标方需具备丰富的等级测评项目经验，参与本项目的测评师不少于4人，必须提供1名参与本项目的高级测评师DJCP的资质证明或ISO27001主任审核员的资质证明。

投标方近三年具备1个以上500kV电压等级厂站电力测评项目案例；出具的报告需满足江西省等保办及属地公安局的要求，需要加盖等级保护专用章或CNAS检验机构公章。

3.1.2投标方不得以任何形式分包、转包。

3.1.3投标方应提出需要甲方配合的工作事项。

3.1.4 投标方提供协助电力监控系统的备案工作。

3.1.5本项目为总承包工程，投标方负责项目技术服务费、技术资料、设计联络、咨询费、现场评审会议费用，承包商邀请专家人员（人员须为省级以上能源局专家库人员）各种费用、税费等所有完成项目所需的一切相关费用。

* 1. **对投标方的技术要求**

投标方除了应具备招标公告中对“合格投标方”要求的资质以外，还应达到如下要求：

对于已经过验收合格的最近实施的类似项目，应提供项目名称及项目单位名称、项目单位地址、联系人及电话、项目实施时间、项目规模及实施内容、对项目实施过程中所可能产生的各种文档必须做统一描述，包括文档名称、内容、提交用户的时间和方式等。在中标后，应认真组织好技术及管理队伍，做好工作计划并提出长期维护服务和技术支持的措施、计划和承诺。在中标后，应负责在项目完成时将全部有关技术文件和资料、验收报告等文档汇集成册交付业主。 本项目终验完成作为中标人项目全部完成并终止的条件。

* 1. **提交技术方案的基本要求**

（1）投标方应根据本技术规范书的要求阐述对本项目的理解，并提出相应的技术方案。 投标方针对本项目编写的技术方案至少应包括以下内容：项目理解、技术方案、实施方案、项目管理方案、质量保证方案和风险控制方案等内容。若认为存在服务内容漏缺，投标方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。

（2）投标方提供的投标报价，中标后原则上不再作任何调整。投标方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，所产生的费用由投标方承担。

（4）协助被测单位开展信息系统的定级与备案工作

具体要求：根据国家和电力行业信息安全要求，结合电厂实际需求，严格遵循《信息系统安全等级保护定级指南》（GB/T 22240-2020），并应深入调研掌握信息系统的应用部署实际情况，按照国家有关管理规范和标准要求，细致分析各信息系统安全域及管理边界，合理划分信息系统范围，科学开展信息系统重要性程度分析，准确判定信息系统安全等级，编制《定级报告》和《备案表》，并按照定级备案流程，向主管部门、监管机关就信息系统定级进行审批备案，使顺利获得监管机关颁发的《信息系统安全等级保护备案证明》；若备案不成功，则合同不生效。

* 1. **对招标文件技术部分的应答要求**

投标方必须对本技术规范书中要求应答部分作点对点实质性响，其响应与招标文件内容采用同样的顺序。

* 1. **驻场服务人员要求**

投标方应与招标方签订保密协议，对检测和加固过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据侵害招标方的权益，否则招标方有权追究投标方的责任。

投标方工作中的过程和文档，应具有规范性，便于项目跟踪和控制。

* 1. **技术支持服务要求**

测评及评估工作本身也会引入安全风险，必须加强测评及评估过程中的风险控制。项目实施前，双方应充分讨论并明确测评及评估对系统可能带来的风险和隐患，确定测评及评估对象、测评及评估方法和工具，并制定应急恢复措施。

（1）操作的申请和监护

测评及评估操作必须遵守现场运行规章制度，确保系统安全稳定运行。如需在线测试，按照相关工作规程，事前申请，并在专责人员的指导和监护下进行。

（2）人员与数据管理

重视保密工作，加强测评及评估过程中的保密管理，确保参与测评工作人员的可靠、稳定，防止敏感信息泄漏。

（3）测评对象选择

优先选择备用设备（系统）或临时搭建的模拟环境进行测评及评估，避免影响在线系统运行。

（4）制定应急预案

根据被测系统情况，在测评及评估实施前制定应急预案，加强系统在线应急处置能力。

（5）关键业务系统风险控制

生产控制大区在线运行系统禁止采用渗透测试工具进行测评。

1. **工程管理**
   1. **工程和服务需求**

（1）投标方应提供工程施工与系统实施服务的详细方案，方案中应分别描述施工与系统实施的具体工作内容、投入人员、人员简介、工作日程表等内容。日程表应涵盖方案设计、现场测评、报告分析和编制、项目验收技术培训等方面。

（2）中标方应向用户单位提供产品和服务，承担方案中的所有设备及软件的集成责任，无论该设备或软件是由中标方采购还是招标方提供的设备。承诺与本项目的相关单位进行积极主动的合作。

（3）投标方应充分重视项目实施过程中的安全管理（包括人员安全、设备安全、信息安全等） ，提出明确的安全管理措施。

（4）投标方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。投标方的项目组织机构中应包含实施本项目所必须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它工作。

（5）投标方应在中标后负责在项目规定的时间内完成项目实施工作内容。

* 1. **技术支持和售后服务**

（1）投标方在中标后，应根据招标方的要求提供现场技术支持与售后服务。投标方必须承诺至少提供以下的技术支持与售后服务，并在应答时应详细阐述技术支持与售后服务的内容和范围。

（2）投标方应提供针对本项目的技术支持与售后服务方案，该方案中还应包括完整的系统运行维护方案，以保证系统的安全稳定运行。

（3）投标方必须对业主方所提出的系统维护要求做出实质性响应，提供各种突发事件的应急策略（包括具体响应时间）。投标方应详细列出服务方案和系统应急方案，一经应答将作为合同的一部分。

（4）本招标项目售后服务期为1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。提供 7X12 小时售后服务电话技术支持。

* 1. **项目验收及考核**

验收应按照招标方确认的验收测试大纲进行，全过程必须由招标方在场见证。

* 等级保护测评及安全防护评估项目目标是输出等级保护测评及安全防护评估报告，该项目将产生一定数量的文档。
* 投标方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。
* 投标方应提交验收流程、验收方法和验收依据。
* 投标方应提供交付件归档办法和方式。
* 投标方应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。大纲必须经招标方确认后方可生效。
* 验收报告需双方代表签字认可。
* 电力监控系统安全防护评估报告如未在2021年4月30日前完成，每延期一个工作日，按5000元/天考核。（甲方整改原因除外）
* 等级保护测评及安全防护评估工作无法满足技术要求，按500元/项考核。（仅限于现有技术标准情况下）
  1. **项目文档**
     1. 投标方提供的资料应使用国际单位制（SI），语言为中文。
     2. 资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整。如所供资料不能达到要求时，投标方应免费给予补充。
     3. 投标方资料的提交应及时充分，满足项目进度要求。
     4. 投标方完成项目后应提供至少6份纸质版（加盖服务机构公章）及电子版文档，具体文档（不仅限于）如下：

表3-1 投标方完成项目提供文档列表

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **文档名称** | **提交时间** | **备注** |
| 1 | 《测评方案》 | 签署合同后1周 | 电子版 |
| 2 | 《系统自查指南》 | 签署合同后1周 | 电子版 |
| 3 | 《XXX系统安全等级保护测评报告》 | 现场测评后3周 | 正式版 |
| 4 | 《XXX系统安全等级保护测评报告》 | 现场测评后3周 | 正式版 |
| 5 | 《XXX系统安全等级保护测评报告》 | 现场测评后3周（加盖DJCP及CNAS公章） | 正式版 |
| 6 | 《电力监控系统安全防护评估报告》 | 现场测评后1周（加盖DJCP及CNAS公章） | 正式版 |
| 7 | 《系统安全加固服务报告》 | 现场测评后3周（加盖CNAS公章） | 正式版 |
| 8 | 《整改建议书》 | 现场测评后3周（加盖CNAS公章） | 正式版 |

* 1. **质量保证**

投标方在项目方案设计、实施、验收的各个阶段，均应满足电力监控系统正常稳定运行的要求。

投标方出具的相关报告应得到行业主管单位认定。

* 1. **保密要求**

投标方承担被测评及评估单位敏感信息的保密责任，在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。

未经双方书面同意，不得向第三方透露项目和涉及双方企业信息安全、技术成果的任何内容。

项目结束后，双方必须互相确认测评过程中提供的相关资料，相互承担保密责任。