



毕节供电局电力监控系统网络安全 防护设备完善项目 技术规范书

贵州电网有限责任公司

2022. 8 贵阳全部



1. 总则

本技术规范为毕节供电局电力监控系统网络安全防护设备完善项目技术规范。投标方必须仔细阅读本技术规范的所有条款，以中文逐条做出明确答复（点对点应答）并给出相关技术指标偏差，提供技术建议书，提交设备配置清单及相关产品详细说明文档，及具体实施计划等附件资料。

本技术规范描述了所需专用设备的技术参数，定义安装、测试和验收的细节和规范，明确对投标方在售后服务、培训服务、技术文档方面的要求，供投标方编写建议书和报价之用（建议书的内容格式应符合本规范书的要求）。投标方应针对自己的特点，根据本规范所描述的专用设备的具体要求，提供符合要求的产品。

本技术规范适用于毕节供电局电力监控系统网络安全防护设备完善项目的物资采购、验收调试、交付、现场安装和试验的指导、监督以及试运行工作。现场安装和试验在招标方的指导和监督下由投标方完成。

本技术规范所描述的各种功能、性能需求仅供投标方编制投标文件之用。投标方可以提出不同的建议方案，但是建议方案必须满足但不限于本标书所阐述的全部技术功能要求。

本标书仅描述基本的技术需求，不保证对一切技术细节做出规定，也不保证已充分引述有关标准和技术条文，投标方须根据需求目标提供进一步具体的可满足要求的功能和性能指标。

本招标技术文件经买、卖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法律效力。

投标方应具备在贵州电网有限责任公司的当地服务提供能力。同时，软件原厂商应提供书面承诺，保证如中标方不能履行合同时，由原厂商无条件继续履行，且承担相应法律、商务及技术责任。

投标方所提供的组件或附件如需向第三方外购时，投标方应对质量向招标方负责，并提供相应出厂和验收证明。

招标方针对投标方所提供的技术服务质量将在中标后的产品供货、项目实施、验收、运行维护支持等阶段工作中进行考核评价，并将会把该考核评价结果计入下一年度的设备招标评价中，投标方应确保针对本次招标的服务承诺为真实可信

的承诺标准，否则招标方保留进行追责和索赔的权利。

投标方提供的产品具有先进性、可靠性和可扩展性，并具有较高的性能价格比。

投标方提供的各项软件产品的特点、性能应完全符合招标方指明的标准，并满足或高于招标方提出的要求。

如果投标方提供的产品与本招标技术条件书的要求有差异，应在投标书中以“技术偏差”为标题的专门章节中加以详细描述。投标方如不能满足本招标技术条件书的要求部分，也应在技术建议书中提出说明。

招标采购单位在任何时候发现投标人提交的投标文件内容有下列情形之一时，将取消其投标或中标资格，并保留进一步依法追究投标人责任的权利：

1) 提供虚假的资料（包括但不限于投标人在其投标文件中提供虚假的资格证明文件、业绩证明文件、剩余生产能力表、试验报告等）；

2) 在实质性方面失实（包括但不限于投标人在其投标文件中提供的产品技术参数等与事实不符或虚假应答等）。

投标方建议的技术方案及软、硬件系统配置应符合有关标准（例如 ISO 标准、IEC 标准、ITU-T 建议、GB 标准和 IETF 建议等），投标方若不作说明，则视为符合上述标准。若投标方的设备包含有自己专用标准，应在项目建议书中具体说明，并附上相应的详细的技术资料。

投标方应承诺所提供的设备本身不能有任何安全隐患，对此应承担终身责任。任何由产品安全引起的招标方的信息安全事件，投标方应承担连带责任。

本招标技术条件书应视为保证系统运行所需软件产品与服务的最低要求，如有遗漏，投标方应予以补充，否则一旦中标将认为投标方认同遗漏部分并免费提供。

对于有授权使用数量限制的软件，投标方应书面标出其基本配置可以合法使用的安装用户数量、使用级别和并发用户使用数量及单价，详细说明每个模块授权数量的价格计算方法，以后再增加用户数的价格计算方法，以及各种用户权限数之间的关系。若投标方没有明确表述告知或对招标方隐瞒，造成招标方少配、漏配、错配，导致授权数量、具体使用权限方面的版权纠纷，投标方应付全部责任。

投标方未经招标方同意，不得以任何形式向第三方公开本招标技术条件书。

本招标技术条件书未尽事宜，由招投标双方在合同履行阶段协商确定，或以其他招标文件（如合同模板，下同）规定为准；与其他招标文件冲突的，以本技术规范书为准；与其他招标文件同类要求标准不一致的，以标准较高为准。

本招标技术条件书解释权属招标方所有。

2. 质量及安全保证

投标方应保证制造过程中的所有工艺、材料等（包括投标方的外构件在内）均应符合协议书的规定。若招标方根据运行经验指定中标方提供某种外购零部件，中标方应积极配合。

中标方提供的任何固件和软件不得存在漏洞和后门。

中标方所提供固件和软件的原制造商应提供补丁支持。

中标方或中标方所提供固件和软件的原制造商发现缺陷，应在发布补丁程序后一周内向招标方提供补丁程序。

招标方发现中标方所提供固件和软件存在缺陷，原制造商应在接到招标方通知之日起 1 个月内提供相应的补丁程序。

中标方要确保供货范围完整，需满足本技术规范的供货要求及技术、功能、性能等要求，并以能满足用户安装、运行要求为原则。若签订合同后，在安装、调试、运行中发现缺项，则由中标方负责免费补充。

3. 项目综述

3.1 项目目标

本次项目建设目标：在毕节地调 OCS 系统 III 区边界部署 web 应用防火墙（WAF）、入侵防御装置（IPS），为毕节电网电力监控系统网络安全运行管理提供基础软硬件支撑。

3.2 投标方应遵循的标准

投标人提供的文件、计算、图纸中的单位均采用国际标准单位。投标方

所提供的应遵循以下法规及技术标准规范（如有最新版本遵循最新版本），包括但不限于：

- (1) 《中华人民共和国网络安全法》
- (2) 《中华人民共和国密码法》
- (3) 《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令 147 号）
- (4) 《电力监控系统安全防护规定》（国家发展和改革委员会令 2014 年第 14 号）
- (5) 《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）
- (6) 《电力监控系统安全防护评估规范》（国能安全〔2015〕36 号）
- (7) 《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318 号）
- (8) 《电力行业网络与信息安全管理办法》（国能安全〔2014〕317 号）
- (9) 《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）
- (10) 《信息安全等级保护管理办法》（公通字〔2007〕43 号）
- (11) 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
- (12) 《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）
- (13) 《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）
- (14) 《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）
- (15) 《信息安全技术网络安全等级保护测评技术要求》（GB/T 28448-2019）
- (16) 《信息安全技术信息安全风险评估规范》（GB/T 20984-2016）
- (17) 《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451 号）
- (18) 《中国南方电网电力调度管理规程》（Q/CS212045-2011）
- (19) 《中国南方电网电力监控系统安全防护技术规范》
- (20) 《中国南方电网电力监控系统网络安全管理办法》（Q_CSG2072003-2021）

这些标准提出了最基本要求，如果根据投标方的意见并经招标方接受，使用优于或更为经济的材料和服务，并能使投标方良好地、连续地在本规范所规定的条件下运行时，则这些标准也可以由投标方超越。

当标准、规范之间出现矛盾时，以较高标准执行，同时投标方应将矛盾情况提交招标方。

3.3 采购清单

具体规格、数量见设备材料清册。

4. 技术要求

以下标注“★”的条款为关键参数，须提供原厂商加盖公章的功能承诺函（招标方保留功能测试查验权利），评标过程中将重点关注。

4.1 性能要求

产品类型	指标项	参数要求
WAF	规格配置	★标准机架设备,1个HA口,1个RJ-45 Console口,1个10/100/1000 Base-T 带外管理口,4个业务电接口（电接口支持 bypass）,4个业务光口,2个网络接口板扩展槽位（最大可扩展16个千兆接口）,2个USB口,双电源。
	性能要求	★网络层吞吐率不少于8G,最大HTTP并发连接数不小于400万

产品类型	指标项	参数要求
IPS	规格配置	★标准机架设备,1个HA口,1个RJ-45 Console口,1个10/100/1000 Base-T 带外管理口,4个业务电接口（电接口支持 bypass）,4个业务光口,2个网络接口板扩展槽位（最大可扩展16个千兆接口）,2个USB口,双电源。
	性能要求	★网络层吞吐率不少于8G,最大并发连接数不小于400万

4.2 功能要求

产品类型	指标项	参数要求
WAF	功能要求	(1) 支持获取 Web 安全事件的原始攻击信息,提供加盖原厂商公章的界面截图证明文件。

		(2) ★系统应支持未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等。提供加盖原厂商公章的界面截图证明文件。 (3) ★系统支持密码穷举探测功能，提供至少 16 种应用的密码穷举行为探测和阻断。同时，系统还应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 4 个不同级别的扫描容忍度/扫描敏感度。提供加盖原厂商公章的界面截图证明文件。 (4) 具备 Web 恶意扫描防护的检测与防御能力，提供加盖原厂商公章的界面截图证明文件。 (5) ★支持自定义事件升级内容。针对新增加的事件特征，针对不同级别的事件，用户可以选择是否自动升级到自定义策略中。升级界面中至少包含高中低三种级别事件的升级启用选项。提供加盖原厂商公章的界面截图证明文件。 (6) 支持获取 Web 安全事件的原始攻击信息，提供加盖原厂商公章的界面截图证明文件。 (7) 具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截，提供加盖原厂商公章的界面截图证明文件。 (8) 系统支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步。系统应支持软硬件 Bypass 功能。提供加盖原厂商公章的界面截图证明文件。
--	--	--

产品类型	指标项	参数要求
IPS	功能要求	(1) 系统入侵防御事件库事件数量不少于 5000 条。 (2) ★系统应支持未知 C&C 通道（隐蔽通道）检测功能，能够提供 C&C 通道的危险级别、连接建立时间、连接持续时间、控制端 IP 地址和端口、受控端 IP 地址和端口等 C&C 通道信息。提供各种响应动作：阻断会话、临时阻断和抓包分析等。提供加盖原厂商公章的界面截图证明文件。 (3) ★系统支持密码穷举探测功能，提供至少 16 种应用的密码穷举行为探测和阻断。同时，系统还应支持多种防 web 扫描能力，包括爬虫、CGI 和漏洞扫描等，并支持设置至少 4 个不同级别的扫描容忍度/扫描敏感度。提供加盖原厂商公章的界面截图证明文件。 (4) 针对 SQL 注入和 XSS 攻击，设备应提供在线事件分析功能，至少提供攻击方法、攻击字段和攻击域、影响的数据库等。提供加盖原厂商公章的界面截图证明文件。 (5) ★支持自定义事件升级内容。针对新增加的事件特征，针对不同级别的事件，用户可以选择是否自动升级到自定义策略中。升级界面中至少包含高中低三种级别事件的升级启用选项。提供加盖原厂商公章的界面截图证明文件。

		(6) 系统应支持本地日志及日志外发，支持与南网统一安全审计系统进行联动，需提供联动机制技术说明。提供加盖原厂商公章的界面截图证明文件。 (7) 系统应支持单独的恶意样本检测规则升级功能，方便对恶意样本检测功能进行扩充。系统应支持恶意样本自学习功能，除通过网络文件捕获外，还支持通过系统直接上传文件，自动识别黑白文件并提供简要信息。提供加盖原厂商公章的界面截图证明文件。 (8) 系统支持双机热备和双机主备功能，并且主备热备时需支持连接状态和配置同步。系统应支持软硬件 Bypass 功能，通过 CPU 和内存阈值实现软件 Bypass 的开启，光口支持外界 Bypass 设备，提供不同的阈值计算方式（最高值/平均值、时间区间等）。提供加盖原厂商公章的界面截图证明文件。
--	--	---

4.3 安全要求

产品类型	指标项	参数要求
WAF	安全性要求	(1) ★投标产品具有《计算机信息系统安全专用产品销售许可证》，销售许可证为 WAF 国标-增强级，提供证书复印件及盖公章。 (2) 投标产品具有网络关键设备和网络安全专用产品安全认证证书。提供加盖原厂商公章的证书扫描件。 (3) 投标产品具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，并获得 EAL3+级别。提供加盖原厂商公章的证书扫描件。 (4) ★产品制造商须为 CNNVD 一级支撑单位。提供加盖原厂商公章的证书扫描件。 (5) ★原厂商为网络安全应急服务支撑单位（国家级），提供原厂商盖章的证明材料。

产品类型	指标项	参数要求
IPS	安全性要求	(1) ★投标产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，提供加盖原厂商公章的证书扫描件。 (2) 投标产品具有中国信息安全认证中心颁发的《中国国家信息安全产品认证证书》。提供加盖原厂商公章的证书扫描件。 (3) 投标产品具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，并获得 EAL3+级别。提供加盖原厂商公章的证书扫描件。 (4) ★产品制造商须为 CNNVD 一级支撑单位。提供加盖原厂商公章的证书扫描件。 (5) ★产品制造商为网络安全应急服务支撑单位（国家级），提供原厂商盖章的证明材料。

5. 保密要求

供需双方均应承担保密责任，在项目实施过程前双方应签订保密协议，明确双方责任义务。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。

6. 验收

验收分为到货验收、功能验收。所有验收工作由甲方组织进行。

6.1 到货验收

1) 设备和技术文件到达交货地点后，甲、乙双方共同对其进行检查，并认真做好交接记录，各方签字。确保软件产品和技术文件的数量、名称与合同要求的清单核实无误。

2) 甲方如发现乙方所提供产品的规格、数量等与合同规定不符，乙方须按合同要求更换或是补足与合同不符的或是短缺的产品，并承担由此而产生的一切费用。

3) 所进行检查的结果符合合同中的规定时，由甲、乙双方共同签署到货验收报告。

6.2 功能验收

1) 到货验收完成后，乙方须完成合同产品的安装、调试等工作。确保乙方提供的软件产品功能与合同要求内容一致，且能稳定、可靠的运行使用。

2) 若验收内容均达到验收标准，则功能验收通过，乙方须撰写并提交功能验收报告，并将所有系统配置的有关资料整理移交甲方，甲、乙双方共同签署功能验收报告。

7. 技术文件要求

投标方提供的技术文件包括：

- 1) 实施安装、调试、测试、验收、培训阶段的文件、图纸，及设备操作维护手册等。
- 2) 每次维护（包括硬件及软件）的维护报告及技术文档。
- 3) 投标方采购供货的第三方设备的技术手册及相关资料。
- 4) 投标方应对其所提供的全部文档的准确性和完整性负责。所有由投标方采购供货的第三方设备的技术手册的准确性由投标方负责。
- 5) 设备应附有完整的、装订好的安装图和说明手册，随设备装箱一起运至现场。
- 6) 投标方至少提供技术文件资料电子版 2 份，以只读光盘和 U 盘形式各提供 1 份；纸质形式打印稿 4 份。文字部分采用 Microsoft Office 2003 格式（包括 Word, Excel, PowerPoint 等文件格式），图纸部分采用 AUTOCAD R14/2000 或 Visio 2003 格式。

8. 监造、包装、运输、安装及质量保证

- 1) 设备制造完成并通过试验后应及时包装，否则应得到切实的保护，确保其不受污损。
- 2) 所有部件经妥善包装或装箱后，在运输过程中尚应采取其它防护措施，以免散失损坏或被盗。
- 3) 在包装箱外应标明需方的订货号、发货号。
- 4) 各种包装应能确保各零部件在运输过程中不致遭到损坏、丢失、变形、受潮和腐蚀。
- 5) 包装箱上应有明显的包装储运图示标志（按 GB/T 191-2008）。
- 6) 整体产品或分别运输的部件都要适合运输和装载的要求。
- 7) 随产品提供的技术资料应完整无缺。
- 8) 订购的新型产品除应满足本招标技术文件外，投标方还应提供产品的鉴定证书。

9) 投标方应保证制造过程中的所有工艺、材料等（包括投标方的外购件在内）均应符合本招标技术文件的规定。若招标方根据运行经验指定投标方提供某种外购零部件，投标方应积极配合。

10) 投标方应遵守本招标技术文件中各条款和工作项目的 ISO9000、GB/T19000 质量保证体系，该质量保证体系已经过国家认证和正常运转。

11) 投标方并应做出承诺保证。在质保期内，免费进行维修、更换损坏设备以及对设备和软件的维护等。在质保期内，应提供 7×24 小时的服务；如发生设备或部件硬件故障，应该承诺在 3 个工作日内完成备件的更换，本项要求的满足情况将作为评标的重要依据之一。

12) 柜内的各种元件，应选择具有生产许可证的专业制造厂家的产品。

13) 交货期：合同签订后 30 个工作日。

14) 交货地点：贵州电网有限责任公司电力调度控制中心。

9. 现场服务及售后服务

9.1 现场服务要求

1) 投标方应派出足够的技术人员到现场负责安装、调试、测试、验收、试运行，并负责解决合同设备制造及性能等方面的有关问题，详细解答合同范围内招标方提出的问题。

2) 在产品质保期内有制造质量的设备，由投标方负责修理或更换。对非投标方责任造成的设备损坏，投标方有优先提供配件和修理的义务。

3) 对招标方选购的与本合同设备有关的配套设备，投标方有提供技术配合的义务，并不由此而增加任何费用。

4) 投标方到招标方现场进行设备安装及维修人员必须为其正式员工。

5) 现场工作过程中，现场服务人员应保持固定，除非获得项目单位允许，否则供应商不可对人员进行调整。

9.2 售后服务要求

1) 在承诺的质量保证期内，投标方应提供 7×24 小时的技术支持服务，提供固定的技术负责人及联络电话、传真号码、e-mail 地址等。

2) 质保期内硬件故障时，投标方必须在用户提出维护要求的 4 小时内作出响应，所提供的替代硬件设备的性能应等于和高于原产品的性能，24 小时内故障应得以解决。

3) 在承诺的质量保证期内，投标方应免费提供系统软件升级、培训、设计联络、技术服务，优惠提供有关扩建工程的软件扩容服务。

4) 在用户发现软件故障时，投标方必须在用户提出维护要求的 2 小时内作出响应，12 小时内提交故障分析报告和解决方案，24 小时内故障得以解决。

5) 对于用户提出的软件性能提高、功能增加等改进要求，如属“招标技术文件”或“合同”的范畴，投标方应在 2 周内予以解决；如属“招标技术文件”或“合同”以外的功能开发，也应提供优惠服务。

9.3 培训

1) 投标方应由资深系统研发专家为招标方的技术人员开设现场培训课程。招标方的技术人员应在设备安装调试、运行维护等各方面得到培训，熟悉和掌握运行、检查、修理和维护相关设备并掌握软件开发工具。

2) 投标方应向受训人员提供技术资料、图纸、参考材料、培训手册等；还应提供测试设备、工具和安全设备，以及其它必需品和工作场地。