**福建福海创石油化工有限公司**

**2024年入侵检测系统和安全审计系统设备特征库维护服务项目**

**发包说明**

**一、供货范围**

根据《国家电网公司关于加快推进电力监控系统网络安全管理平台建设的通知(国家电网调〔2017〕1084 号)》和《国网福建电力调控中心关于印发福建电网厂站调度自动化系统可研、初设技术审查要点（试行）的通知》要求，220kV总降站于2019 年增加网络安全监测装置、入侵检测系统和安全审计系统。目前设备特征库程序证书已临近过期，为持续改善和提升涉网设备网络安全状况，避免影响网络安全等级测评。拟委托有相应资质、能力和经验的公司承担以下项目的采购和现场服务等工作任务：

特征库名称

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **产品描述** | **型号** | **数量** | **单位** | **序列号** | **包含以下模块** |
| 1 | 网络入侵检测系统装置 License | NID SNX3-N300A | 5 | 套 | 17-38-L-0669 | 1.1、含引擎软件更新； 1.2、系统规则库； 1.3、病毒库。 |
| 17-38-L-0670 |
| 18-16-L-0144 |
| 19-35-L-0247 |
| 19-42-L-0647 |
| 2 | 工控安全审计装置 License | SAS-ICSNX3-300A | 5 | 套 | 17-39-L-0095 |  |
| 17-39-L-0096 |
| 18-21-L-0158 |
| 19-35-L-0201 |
| 19-38-L-1073 |

**二、技术要求**

2.1 项目承担方资质、业绩要求

（1）投标方须为中华人民共和国独立法人资格；具有完善的质量保证体系及其质量认证证明等；

(2) 投标方须提供营业执照复印件并加盖公章。

（3）投标方需具备熟悉网络入侵检测系统装置及工控安全审计装置的维护能力，并提供近三年完成同类型服务业绩（如：签字盖章的封面及设备型号，至少3份）。

（4）现场已安装网络安全监测、网络入侵检测装置、工控安全审计装置，为避免后续与设备厂家发生纠纷，网络入侵检测系统装置及工控安全审计装置证书服务需提供设备原厂出具授权服务承诺函。

（5）对5台网络入侵检测装置的规则库对进行升级，具体要求如下：

* 提供授权证书license,更新设备维保期，提供规则库升级功能；
* 更新后设备支持 Zoho ManageE ngi ne OpManager cachestart 目录遍历（CVE-2020-13818） 检 测规 则 ；
* 更新后设备支持Mi crosoft Windows Installer 远程代码执行 漏洞(CVE-2020-0814)检 测 规 则；
* 更新后设备支持Mi crosoft Windows Modules Installer Service信息泄露 漏 洞(CVE-2020-0728)检 测规 则 ；
* 更新后完善引擎 、提 高 系统 稳 定性 、优化 web界面访问 速 度,优化syslog日 志自 定 义配 置 等功 能 ；

（6）对5台工控安全审计装置（绿 盟SAS-ICSNX 3-300A）的规则 库对进行升级,具体要求如下 ：

* 提供授权证书license ,更新设备维保期 ,提供操作行为监控功能；
* 更新后设备支持自定义工控协议监听功能 ,解析不同工业厂商私有协议；
* 更新后完善引擎 、提高系统稳定性 、优化 web界面访问速度，优化syslog日志自定义配置等功能 ；
* 更新后设备支持威胁行为监测告警，及时发现敏感威胁 ,并记录。

2.2 物项技术要求

2.2.1 通用技术要求

（1）需派专业技术人员赴现场完成以上设备特征库升级调试，与电网调度中心对接调试并负责对需求方人员进行培训。

（2）所提供的软件或设备需满足“国家电网公司关于加快推进电力监控系统

网络安全管理平台建设的通知，国家电网调[2017]1084 号”文件要求。

（3）需对网络入侵检测装置及工控安全审计装置设备进行网络安全加固，并满足“国家能源局-《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 号文）”以及《国调中心关于开展清朗有序安全网络空间创建活动的通知》（调网安〔2018〕37 号）等 文件要求。

（4）相关证书、软件等物资需满足原厂原型号，匹配其原有配置和应用。

（5）若电网有新的规范要求，以电网最新规范要求为准。

2.2.2 现场服务

项目承担方根据需求方技术要求完成所委托项目的物资采购、现场实施。现场实施工作包括现场施工准备、现场实施、调试验证，以及施工及验证过程中的

各种配合任务等。

**三、现场服务时间**

合同签订后五天内完成现场全部工作，如因发包人原因导致工期延后，经双方友好协商确认后顺延完工日期。

**四、设备特征库授权服务周期**

2024年11月01日～2025年10月31日

**五、 双方职责**

5.1 将需求变更信息及时反馈给项目承担方；

5.2 为采购设备的技术澄清提供支持；

5.3 负责组织对项目承担方单位和人员进行资质验证，以确保项目承担方资质

和经验以及项目承担方参与项目人员的技术能力及水平满足需求方技术要求，若在项目执行过程中发现项目承担方资质不满足要求，及时向项目承担方提出整改要求或清退；

5.4 需求方负责对项目承担方项目进行独立的质保监督，委派专业人员见证项

目各个阶段的关键点，确保项目承担方项目严格按照双方的约定推进，确保项

目的安全质量进度满足双方合同约定，必要时可要求项目承担方停工整改。