**福建福海创石油化工有限公司**

**电力监控系统密码测评服务**

**发包说明**

**2024年07月28日**

**目录**

[1. 概要说明 3](#_Toc160616423)

[2. 密码应用需求 4](#_Toc160616424)

[3. 承包商资质要求 4](#_Toc160616424)7

[4. 工程量清单 27](#_Toc160616425)

[5. 计划开工和完成时间 28](#_Toc160616426)

[6. 服务要求 28](#_Toc160616427)

[7. 质量保证 29](#_Toc160616428)

[8. 保密要求 29](#_Toc160616429)

[9. 考核细则 29](#_Toc160616430)

[10. 违约解除条款 30](#_Toc160616431)

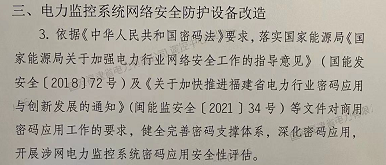
[11. 技术文件交付 31](#_Toc160616432)

# 1. 概要说明

**1.1 基本概况**

2021年9月24日，国网福建电力调控中心下发的《调自〔2021〕132号　国网福建电力调控中心关于直调电厂2022年度调度自动化涉网重点工作安排的通知》中的第三大点的第3小点要求，健全完善密码支撑体系，深化密码应用，开展涉网电力监控系统密码应用安全性评估。

引用原文截图如下：



并且依据《密码法》及《信息安全等级保护商用密码技术要求》的要求，信息系统在投入运行前，必须通过国家密码管理局授权的安全测评机构进行的商用密码应用安全性评估，投入运行后每年需进行评估；以《商用密码应用安全性评估测评作业指导书（试行）》等为指导性文件，指导测评机构规范有序开展评估工作。公安部〔2020〕1960号文也规定信息系统等保测评时需具备相应密评报告。为响应国家能源局相关指示、闽监能安全〔2021〕34号文、《调自〔2021〕132号　国网福建电力调控中心关于直调电厂2022年度调度自动化涉网重点工作安排的通知》及福建省密码局相关文件要求，通过商用密码安全性评估工作，以评促改，进一步提升福建省能源企业的密码应用水平。

根据华电集团下发的《2022年范的要求，同步规划、同步建设、同步运行密码保障措施，制定密码应用方案，定期开展商用密码应网络安全“春季”自查专项检查表》中，建设安全管理下的系统运行期间安全的要求：等保第三级及以上系统，应当落实国家密码管理有关法律法规和标准规用安全性评估，未通过评估的，应当在整改后开展系统验收。如发生密码应用重大调整等情况，主管单位应当及时开展密码应用安全性评估。

**1.2依据和标准文件**

1.2.1《中华人民共和国网络安全法》

1.2.2《中华人民共和国密码法》

1.2.3《商用密码管理条例》

1.2.4 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》

1.2.5 GM/T 0115-2021《信息系统密码应用测评要求》

# 2. 密码应用需求

**2.1 基本情况**

电力监控系统是对电力生产过程进行实时监视、数据采集和远程控制的基于计算机及网络技术的业务系统和智能设备，其功能主要包括数据通信、数据釆集和处理、运行监视和事件报警、人机联系和操作控制、安全分析等功能。站内电力监控系统主要为配合远方调度工作的调控系统终端及本地就地数据浏览功能。

**2.2 系统网络拓扑**

。

**2.3 测评实施方案**

**2.3.1 密评依据**

2.3.1.1 《中华人民共和国密码法》、《中华人民共和国网络安全法》、《国家政务信息化项目建设管理办法》、《商用密码应用安全性评估管理办法（试行）》。

2.3.1.2 有关国家技术规范和标准，包括但不限于：

《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；

《信息系统密码应用测评要求》（中国密码学会密评联委会2020年12月）；

《信息系统密码应用测评过程指南》（中国密码学会密评联委会2020年12月）；

《信息系统密码应用高风险判定指引》（中国密码学会密评联委会2020年12月）；

《商用密码应用安全性评估量化评估规则》（中国密码学会密评联委会2020年12月）；

《公安机关商用密码应用指南（试行）》；

《信息安全技术 个人信息安全规范》（GB/T 35273-2020）

《信息安全技术 传输层密码协议（TLCP）》（GB/T 38636-2020）

《SM4分组密码算法》（GM/T 0002-2012）

《SM2椭圆曲线公钥密码算法》（GM/T 0003-2012）

《SM3 密码杂凑算法》（GM/T 0004-2012）

《随机性检测规范》（GM/T 0005-2012）

《SM2 密码算法使用规范》（GM/T 0009-2012）

《数字证书认证系统密码协议规范》（GM/T 0014-2012）

《基于SM2密码算法的数字证书格式》（GM/T 0015-2012）

《IPSec VPN 网关产品规范》（GM/T 0023-2014）

《SSL VPN网关产品规范》（GM/T 0025-2014）

《安全认证网关产品规范》（GM/T 0025-2014）

《智能密码钥匙技术规范》（GM/T 0027-2014）

《密码模块安全技术要求》（GM/T 0028-2014）

《签名验签服务器技术规范》（GM/T 0029-2014）

《服务器密码机技术规范》（GM/T 0030-2014）

《信息系统密码应用基本要求》（GM/T 0054-2018）；

《信息系统密码测评要求（试行）》；

《商用密码应用安全性评估测评过程指南（试行）》；

《商用密码应用安全性评估测评作业指导书（试行）》；

《综合布线的有关国家和行业标准》；

《中华人民共和国通信行业标准》；

《中华人民共和国建设部标准》；

《中国工程建设标准化协会标准》；

《软件开发的国际、国家有关标准和规范》；

《网络质量、安全控制等国际、国家和行业标准》

**2.3.2 评估内容与对象**

依据《信息系统密码应用基本要求》（GM/T0054-2018）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《公安机关商用密码应用指南（试行）》开展商用密码应用安全性评估，从总体要求、物理和环境、网络和通信、设备和计算、应用和数据、密钥管理、安全管理等方面开展评估。

本次评估对象为龙口火电厂电力监控系统（220kV总降站电力监控系统）涉网部分。

根据被测信息系统的重要程度及其相关设备和组件等情况，明确核心资产在被测信息系统内的流转，从而确定与密码相关的测评对象。

被测单位需要确定被测信息系统需要保护的核心资产，以及相应的威胁模型和安全策略。核心资产包括业务应用、业务数据或者业务应用的某些设备、组件。核心资产及其他需要保护的配套数据（如审计信息、配置信息、访问控制列表等）、敏感安全参数（主要指密钥）的威胁模型和安全策略等均由被测单位根据密码应用方案、网络安全等级保护定级报告等确定，并由测评方进行核查和评估。

**2.3.3测评方法**

测评方法主要包括：访谈、文档审查、实地察看、配置检查、工具测试。

2.3.3.1 访谈：通过与被测单位的相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认。

2.3.3.2 文档审查：审核被测单位提交的有关信息系统安全的各个方面的文档，如：被测系统总体描述文件，被测系统商用密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，测评委托单位的信息化建设与发展状况以及联络方式；密码应用方案及评审意见，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次评估报告等等。通过对这些文档的审核与分析确认测评的相关内容是否达到安全保护等级的要求。

2.3.3.3 实地察看：现场查看测评对象所处的环境、外观等情况。

2.3.3.4 配置检查：查看测评对象的相关配置。

2.3.3.5 工具测试：根据被测单位信息系统的实际情况，测评人员使用适合的技术工具对信息系统进行测试。

**2.3.4测评工具**

密码应用安全性评估中涉及的测评工具：

2.3.4.1 协议分析工具主要用于对常见通信协议进行抓包、解析分析。捕获解析的协议数据应能够作为测评人员分析评估通信协议情况的可信依据。

2.3.4.2 端口扫描工具主要用于探测和识别被测信息系统中的VPN、服务器密码机、数据库服务器等设备开放的端口服务，以帮助测评人员分析和判断被测信息系统中密码产品和密码应用系统是否正常开启密码服务。

2.3.4.3 逆向分析工具是指在没有源代码的情况下，通过分析应用程序可执行文件二进制代码，探究应用程序内部组成结构及工作原理的工具，一般可分为静态分析工具和动态分析工具。逆向分析工具主要用于对被测信息系统中重要数据保护强度的深入分析。支持对常见格式文件的静态分析，以及对应用程序的动态调试分析。

2.3.4.4 渗透测试工具主要用于对被测信息系统可能存在的影响信息系统密码安全的风险进行检测识别，支持对被测信息系统开展已知漏洞探测、未知漏洞挖掘和综合测评，并尝试通过多种手段获取系统敏感信息。

2.3.4.5 密码测评专用工具用于检测和分析被测信息系统的密码应用的合规性、正确性和有效性的一部分或全部环节。

根据信息系统的实际情况，测评人员采用预定的工具对测评对象进行测试，使其产生特定的行为等活动，察看、分析输出结果，获取证据以证明信息系统的密码应用措施是否有效。可能涉及的测评工具如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 工具名称 | 用途 |
| 1 | Wireshark | 抓取网络数据包，分析网络协议信息 |
| 2 | GmSSL | 密码算法的加解密、签名验签 |
| 3 | 算法和随机数检测系统 | 密码算法正确性检测和随机数的有效性检测 |
| 4 | 数字证书格式合规性检测系统 | 数字证书格式合规性、有效性检测 |
| 5 | 密码算法验证系统 | 实现对密码算法的数据校验 |
| 6 | Zenmap | 端口扫描，用于网络探测和安全审计 |

**2.3.5评估流程**

商用密码应用安全性评估过程包括四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。测评过程工作流程如下图所示。



图6 测评过程工作流程图

2.3.5.1 测评准备阶段

本活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制密评方案做好准备。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 项目启动 | 项目计划书 | 项目概述、工作依据、技术思路、工作内容和项目组织等。 |
| 信息收集和分析 | 完成的调查表格，各种与被测信息系统相关的技术资料。 | 被测信息系统的网络安全保护等级、业务情况、软硬件情况、密码应用情况、密码管理情况和相关部门及角色等。 |
| 工具和表单准备 | 选用的测评工具清单，打印的各类表单，如现场测评授权书、风险告知书、文档交接单、会议记录表单、会议签到表单等。 | 测评工具、现场测评授权、测评可能带来的风险、交接的文档名称、会议记录表单、会议签到表单等。 |

2.3.5.2 方案编制阶段

本活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成密评方案，为实施现场测评提供依据。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 测评对象确定 | 密评方案的测评对象部分。 | 被测信息系统的整体结构、边界、网络区域、核心资产、面临的威胁、测评对象等。 |
| 测评指标确定 | 密评方案的测评指标部分。 | 被测信息系统相应等级对应的适用和不适用的测评指标。 |
| 测试检查点确定 | 密评方案的测评检查点部分。 | 测评检查点、检查内容及测评方法。 |
| 测试内容确定 | 密评方案的单元测评实施部分。 | 单元测评实施内容。 |
| 密评方案编制 | 经过评审和确认的密评方案文本。 | 项目概述、测评对象、测评指标、测评检查点、单元测评实施内容、测评实施计划等。 |

2.3.5.3 现场测评阶段

本活动是开展测评工作的核心活动，主要任务是根据密评方案分步实施所有测评项目，以了解被测信息系统真实的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 现场测评准备 | 会议记录、更新确认后的密评方案、确认的测评授权书和风险告知书等。 | 工作计划和内容安排、双方人员的协调、被测单位应提供的配合与支持。 |
| 现场测评和结果记录 | 各类测评结果记录。 | 访谈、文档审查、实地察看和配置检查、工具测试的记录及测评结果。 |
| 测评结果的确认和资料归还 | 经过被测单位确认的各类测评结果记录。 | 测评活动中发现的问题、问题的证据和证据源、每项测评活动中被测单位配合人员的书面认可文件。 |

2.3.5.4 分析与报告编制阶段

本活动是给出测评工作结果的活动，主要任务是根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》和《信息系统密码应用测评要求》的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成密评报告。

|  |  |  |
| --- | --- | --- |
| **任务** | **输出文档** | **文档内容** |
| 单元测评 | 密评报告的单元测评部分。 | 汇总统计各测评指标的各个测评对象的测评结果，给出单元测评结果。 |
| 整体测评 | 密评报告的单元测评结果修正部分。 | 分析被测信息系统整体安全状况及对各测评对象测评结果的修正情况。 |
| 量化评估 | 密评报告中整体测评结果和量化评估部分，以及总体评价部分。 | 综合单元测评和整体测评结果，计算得分，并对被测信息系统的密码应用情况安全性进行总体评价。 |
| 风险分析 | 密评报告的风险分析部分。 | 分析被测信息系统存在的安全问题风险情况。 |
| 评估结论形成 | 密评报告的评估结论部分。 | 对测评结果进行分析，形成评估结论。 |
| 密评报告编制 | 经过评审和确认的密评报告。 | 概述、被测信息系统描述、测评对象说明、测评指标说明、测评内容和方法说明、单元测评、整体测评、量化评估、风险分析、评估结论和改进建议等。 |

**2.3.6测评指标**

依据《信息系统密码应用基本要求》（GM/T 0054-2018）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）第三级别要求基本指标，测评指标具体如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 测评单元 | | | 测评指标 |
| 技术要求 | 物理和环境安全 | 身份鉴别 | a）宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性； |
| 电子门禁记录数据存储完整性。 | b）宜采用密码技术保证电子门禁系统进出记录数据的存储完整性； |
| 视频监控记录数据存储完整性 | c）宜采用密码技术保证视频监控音像记录数据的存储完整性。 |
| 网络和通信安全 | 身份鉴别 | a）应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性； |
| 通信数据完整性 | b) 宜采用密码技术保证通信过程中数据的完整性； |
| 通信过程中重要数据的机密性 | c) 应采用密码技术保证通信过程中重要数据的机密性； |
| 网络边界访问控制信息的完整性 | d) 宜采用密码技术保证网络边界访问控制信息的完整性； |
| 安全接入认证 | e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。 |
| 设备和计算安全 | 身份鉴别 | a) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性； |
| 远程管理通道安全 | b) 远程管理设备时，应采用密码技术建立安全的信息传输通道； |
| 系统资源访问控制信息完整性 | c) 宜采用密码技术保证系统资源访问控制信息的完整性； |
| 重要信息资源安全标记完整性 | d) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性； |
| 日志记录完整性 | e) 宜采用密码技术保证日志记录的完整性； |
| 重要可执行程序完整性、重要可执行程序来源真实性 | f) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。 |
| 应用和数据安全 | 身份鉴别 | a) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性； |
| 访问控制信息完整性 | b) 宜采用密码技术保证信息系统应用的访问控制信息的完整性； |
| 重要信息资源安全标记完整性 | c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性； |
| 重要数据传输机密性 | d) 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性； |
| 重要数据存储机密性 | e) 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性； |
| 重要数据传输完整性 | f) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性； |
| 重要数据存储完整性 | g) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性； |
| 不可否认性 | h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。 |
| 管理要求 | 管理制度 | 具备密码应用安全管理制度 | a）应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度； |
| 密钥管理规则 | b）应根据密码应用方案建立相应密钥管理规则； |
| 建立操作规程 | c）应对管理人员或操作人员执行的日常管理操作建立操作规程； |
| 定期修订安全管理制度 | d）应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订； |
| 明确管理制度发布流程 | e）应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制； |
| 制度执行过程记录留存 | f）应具有密码应用操作规程的相关执行记录并妥善保存。 |
| 人员管理 | 了解并遵守密码相关法律法规  和密码管理制度 | a）相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度； |
| 建立密码应用岗位责任制度 | b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限：  1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；  2) 对关键岗位建立多人共管机制；  3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任；  4) 相关设备与系统的管理和使用账号不得多人共用。 |
| 建立上岗人员培训制度 | c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能； |
| 定期进行安全岗位人员考核 | d) 应定期对密码应用安全岗位人员进行考核； |
| 建立关键岗位人员保密制度和调离制度 | e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。 |
| 建设运行 | 制定密码应用方案 | a）应依据密码相关标准和密码应用需求，制定密码应用方案； |
| 制定密钥安全管理策略 | b）应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术 信息系统密码应用基本要求》附录A； |
| 制定实施方案 | c）应按照应用方案实施建设； |
| 投入运行前进行密码应用安全性评估 | d）投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行； |
| 定期开展密码应用安全性评估及攻防对抗演习 | e）在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。 |
| 应急处置 | 应急策略 | a）应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置； |
| 事件处置 | b）事件发生后，应及时向信息系统主管部门进行报告； |
| 向有关主管部门上报处置情况 | c）事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。 |

**2.4 测评范围**

龙口火电厂电力监控系统

**2.5技术要求**

2.5.1 概述

开展商用密码应用安全性评估是衡量信息系统安全的重要抓手，是维护网络空间安全、规范商用密码应用的客观要求。通过密码评估，可以有效的检验商用密码应用中存在的突出问题，为重要网络与信息系统的安全提供科学评价方法。通过同步规划、同步建设、同步运行建设密码保障体系措施，逐步规范商用密码的使用和管理，从根本上改变商用密码应用不规范、不安全的现状，确保商用密码在网络与信息系统中的有效使用，切实构建起坚实可靠的网络空间安全密码屏障。

2.5.2 密码需求调研

密码需求调研是信息系统开展密码建设的首要工作，通过对信息系统的资产情况、承载业务情况、网络架构、当前密码应用情况等进行调研。梳理关键密码应用需求，为后续的密码应用方案编写、密码改造方向确认等提供数据支撑依据。

2.5.2.1 信息系统资产调查

根据密码资产调研工作要求，针对目标信息系统的物理环境、物理安防设施、密码产品、服务器/存储设备、网络及安全设备、数据库管理系统、关键业务应用、密码服务、重要数据、安全管理文档、人员信息等进行调研梳理，形成相关报告，并依据信息系统所有相关文档和现场调查结果形成资产汇总材料。

2.5.2.2 密码需求分析

根据密码资产调研工作情况，结合现有的密码建设情况，在信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理及密钥管理层面进行密码需求确认。确定各层面的机密性、完整性、真实性、不可否认性等技术层面密码需求和安全合规的密码管理措施。

2.5.3 密码方案编写

2.5.3.1 密码应用方案内容

总体性原则：密码应用需求和系统预期目标需要与本信息系统的网络安全等级保护相结合。

科学性原则：应遵循GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的密码技术体系框架和密码相关标准。

完备性原则：根据安全需求建立完备的密码支撑保障体系。针对不适用项，指出采用了何种替代性风险控制措施来达到有效控制。

可行性原则：信息系统密码应用设计应进行可行性论证，在保证信息系统业务正常运行的同时，综合考虑信息系统的复杂性、兼容性及其他保障措施等，保证方案切合实际、合理可行。

三大要点

合规性：信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，信息系统中使用的密码技术应遵循密码相关国家标准和行业标准或经国家密码管理部门审查认定，密码产品和密码服务应符合法律法规的相关要求。

有效性：密码技术是否被正确、有效使用以支撑信息系统的安全需求，为信息系统提供机密性、完整性、真实性、不可否认性的保护。

密钥安全管理：指的是对系统中各密钥功能进行分类，明确密钥生命周期，制定科学、合理的密钥安全管理策略。

2.5.3.2 主要内容

结合密码应用方案涉及要求，密码应用方案应包括背景、系统概述、密码应用需求分析、设计目标及原则、技术方案、安全管理方案、实施保障方案等部分。

2.5.3.2.1 通用设计指南要求

根据通用设计指南要求，应用方案设计中应确定密码算法、密码技术、密码产品和密码服务的选取规则。

密码算法和密码技术的选取要遵循标准化和合规化要求。标准化，优先采用以国家标准或密码行业标准形式公开发布的密码算法和密码技术。合规化，在采用特定行业领域的专用密码算法和密码技术前，需要确定该密码算法和密码技术 是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

密码产品和服务的选择要遵循合法合规和级别要求。合法合规，信息系统应采用商用密码认证机构认证合格的密码产品，以及符合法律法规的相关要求并获得国家密码管理主管部许可的密码服务。级别要求，采用的密码产品应满足GB/T 37092对应等保级别要求。

2.5.3.2.2 信息系统密码设计

信息系统应用层设计依赖于具体的业务应用和安全需求需要从业务应用情况入手，梳理信息系统的业务安全需求，明确信息系统的机密性、完整性、真实性、不可否认性要求。通过对信息系统功能、系统架构、业务应用情况、密码应用情况、重要信息资源、软硬件组成和管理机制等现状的分析，了解信息系统业务逻辑,明确业务流转中重要业务数据、隐私数据存储、传输的业务需求，确定需要保护的重要信息资源。

信息系统计算平台的密码应用设计，具体包含物理和环境网络和通信、设备和计算三个层面，保障信息系统计算平台的物理环境、网络通信、设备管理等方面的安全。

密钥管理安全设计主要包括信息系统应用层密钥管理设计，以及密码服务支撑、计算平台密码应用等内容的密钥管理设计。明确密钥体系，并针对密钥体系中的各类密钥，明确支持的生命周期环节及各环节中的安全措施。明确密钥从产生到销毁的全生命周期中的各个环节，确保密钥的安全性。证密钥(除公钥外)不被非授权的访问、使用、泄露修改和替换，保证公钥不被非授权的修改和替换。

密码服务支撑设计包括支撑中间件与密码设备/基础设施的设计。一是支撑中间件，设计密码功能、密码计算等密码服务的提供模式，同信息系统的集成与调用方式等;二是密码设备/基础设施，设计提供密码服务的密码设备、密码基础设施并确定其功能、性能需求及部署模式。

2.5.4 密码管理方案

针对目前系统责任单位的实际情况，制定密码管理要求，包括管理制度，人员管理、建设运行和应急处置。

2.5.4.1管理制度要求：

1)制定安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

2)根据密码应用方案建立相应密钥管理规则；

3)对管理人员或操作人员执行的日常管理操作建立操作规程；

4)定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；

5)明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；

6)对密码应用操作规程的相关执行金记录并妥善保存。

2.5.4.2人员管理要求：

1)建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限；

2)根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位；

2.1)对关键岗位建立多人共管机制；

2.2)密钥管理、密钥安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任；

2.3)相关设备与系统的管理和使用账号不得多人共用。

3)建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；

4)定期对密码应用安全岗位人员进行考核；

5)建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

2.5.4.3建设运行要求

1)依据密码相关标准和密码应用需求，制定密码应用方案；

2)根据密码应用方案，确定系统涉及的密钥种类、体系及生存周期环节，各环节密钥管理要求；

4)在运行过程中，严格执行既定的密码应用安全管理制度，定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

2.5.4.4应急处置要求：

1)制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，立即启动应急处置措施，结合实际情况及时处置；

2)事件发生后，及时向信息系统主管部门进行报告；

3)事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

实施保障方案：根据密码应用及评估过程中的内容，明确项目实施保障方案涉及人员组织保障、实施技术保障、项目质量保障、项目经费保障等。

2.5.5 密码应用改造指导

根据密码应用方案要求，在充分考虑目标信息系统网络安全现状、密码建设情况下，进行密码建设改造。围绕密码应用方案内容，就物理和环境层面、网络和通信层面、设备和计算层面、应用和数据层面开展密码技术的改造和建设。开展相关密码产品和服务的建设、对应用系统进行密码适配对接，确保信息系统的密码改造符合密码应用方案的要求，满足系统在真实性、机密性、完整性和不可否认等要求。

在密码应用改造指导中，提供相关密码产品和服务清单。详细密码建设网络拓扑图密，密码应用改造对接方案等。

在安全管理层面，根据实际情况，结合密码要求，制定密码管理制度和操作管理规程。

2.5.6 密码安全评估

按照GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、GM/T 0115-2021 《信息系统密码应用测评要求》、GM/T 0116-2021 《信息系统密码应用测评过程指南》的要求，为信息系统管理部门提供规范有序开展商用密码应用安全性评估，客观公正出具测评报告。

具体工作服务范围包括：

1)总体要求评估，对信息系统中使用的密码算法、密码技术、密码产品及密码服务是否符合法律、法规的规定，是否符合密码相关国家标准、行业标准的有关要求，是否通过国家密码管理部门核准或许可等进行真实环境下较为细致的评估工作；针对不符合和部分符合项应进行说明。

2)密码技术应用要求评估，对信息系统的物理和环境安全密码应用，网络和通信安全密码应用，设备和计算安全密码应用，以及应用和数据安全密码应用分别进行真实环境下较为细致的评估工作。

3)安全管理要求评估，对信息系统的密码安全管理制度及操作规范、安全操作规范，密码安全管理制度的合理性和适用性，密码管理制度的发布流程等进行较为细致的评估工作。

4)问题分析，针对测评结果中存在的部分符合项和不符合项问题加以描述和分析，其中对于部分符合项进行风险分析，评定风险等级，作为整体评判的依据。

报告编制，根据国家密码管理部门最新发布的报告模板，编制《商用密码应用安全性评估报告》。

技术要求：

在商用密码安全性评估服务过程中，需保障日志完整性，工具需具备高性能日志及行为审计能力。（须提供具第三方权威机构证明材料并加盖公章）

在服务过程中，为确保商用密码安全性评估资产全覆盖，主动发现未知资产，所采用的服务工具提供主动探测服务，可以对IP、域名进行主动探测，探测的结果信息包括IP、端口、协议组件等,可以将资产和相应部门的负责人进行绑定，通过任务触发扫描漏洞，扫描到漏洞存在后，将漏洞信息发送给自定义绑定的相应资产负责人。（须提供第三方检测机构（需通过CMA或CNAS认证）出具的检测报告复印件并加盖公章）

为确保服务过程中全过程可视以及文档留存，所提供的密码测评平台应具备密评过程全流程管理能力，包括系统基本信息管理、资产管理、现场核查记录管理、风险分析管理及测评相关文档归档工作等，提供相关证明材料。

安全评估及培训服务

安全风险评估：根据《国能安全【2015】36号-国家能源局关于印发电力监控系统安全防护方案和评估规范的通知》安全防护评估规范标准对电力监控系统系统进行系统安全防护评估，并提供安全评估报告。

漏扫服务：结合系统当前资产现状，提供漏洞扫描服务，发现系统中存在的安全弱点和安全问题，主要针对服务器、网络安全设备、数据库和中间件等进行漏洞扫描，需提供《漏洞扫描报告》。

资产梳理：结合系统当前资产现状，针对信息资产进行全面梳理，同时对资产数量、资产种类、资产细粒度、资产变化进行分析展现，保障资产管理数据的准确性和价值，最终形成资产台账清单明确责任制。

安全培训：提供的安全意识培训，需要键盘远程控制、U盘入侵等贴近日常工作场景生动展示，保证安全意识培训的质量，有效提高人员意识，需要提供①可远控键盘等设备图片以及功能截图；②安全意识培训：开展一次员工安全意识培训服务，提供贴合日常生活场景中的场景宣传演示:键盘远程控制、U盘入侵等安全场景培训。

勒索攻击排查服务：针对系统当前资产现状，提供专业安全服务，提供从勒索攻击发现到响应到恢复的全链条综合治理方案，提早发现隐患、及时封堵攻击、避免二次勒索，最大化降低受勒索攻击风险和影响。

除此之外，还需提供包含但不限于以下报告：

表6.1

|  |  |
| --- | --- |
| 能力培训 | 《网络安全防护经验分享》 |
| 《网络安全工具培训》 |
| 《攻防技术详解》 |
| 《网络安全防御现状梳理报告》 |
| 《安全防御体系分析报告》 |
| 《防御战术分析》 |
| 《定制化战术详解-互联网暴露面收缩》 |
| 《定制化战术详解-无人机反制技战法》 |
| 《定制化战术详解-增强钓鱼邮件的防护》 |
| 《攻防演练规则详解》 |
| 《网络安全意识提升培训》 |
| 《防守技术培训》 |
| 核心资产管理 | 《核心资产防护状态》 |
| 《核心资产防护现状分析》 |
| 《核心资产攻击有效性分析报告》 |
| 《核心资产事件处置报告》 |
| 《核心资产分析研判方法》 |
| 《核心资产分析研判改进报告》 |
| 《核心资产事件处置分析报告》 |
| 《核心资产安全事件处置效率分析》 |
| 《核心资产安全事件处置报告》 |
| 网络安全管理 | 《网络安全管理体制现状》 |
| 《安全管理体系优化报告》 |
| 《网络安全防御能力优化报告》 |
| 《网络安全长效反馈体系分析报告》 |
| 《网络安全运营评估体系优化报告》 |

# 3.资质要求

3.1 必须具有中华人民共和国独立法人资格。

3.2 为了更好的保证工控系统密码安全项目在服务过程中的质量，保障业务密码安全性，**承包商提供的项目技术经理需具备:职业技能等级证书(密码安全应用员四级及以上)。**

3.3 承包商提供的技术工程师需要具备**工业和信息化人才专业知识测评证书(NITS)。**

3.4为了更好的保证工控系统密码安全项目在服务过程中的质量，保障业务数据安全性，承包商提供的**技术工程师需具备数据安全官证书（CCRC-DSO）。**

3.5需具备**安全生产许可证、电子与智能化工程专业承包贰级及以上证书。**

# 4.工程量清单

针对本次服务，工程量项目清单如下：

| **序号** | **服务名称** | **服务内容** | **数量** | **单位** | **备注** |
| --- | --- | --- | --- | --- | --- |
| 1 | 商用密码安全管理制度建立 | 提供三级系统的商用密码安全管理制度、人员管理、建设运行和应急处置等相关制度建立服务。 | 1 | 次 |  |
| 2 | 商用密码安全咨询服务 | 提供三级系统的商用密码应用咨询，开展密码需求调研、密码应用方案编写及评审、密码改造指导、辅助密码测评工作，最终配合获得测评单位出具的商用密码应用安全性评估报告。 | 1 | 次 |  |
| 3 | 商用密码安全测评服务 | 提供三级系统的商用密码应用测评服务，开展围绕物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面的密码测评工作，出具的商用密码应用安全性评估报告。 | 1 | 次 |  |
| 4 | 设备厂家服务 | 提供原设备厂家现场配合商用密码安全测评现场服务。 | 1 | 次 |  |
| 5 | 安全风险评估及培训服务 | 提供漏扫服务、资产梳理、安全培训、勒索攻击排查等服务，提供相应安全报告等服务。 | 1 | 次 |  |

# 5. 计划开工和完成时间

计划开工时间：2024年9月15日；

计划完成时间：2024年10月15 日；

计划总工期： 30天。

本次项目所需（物资、设备、人员）要求于合同签订后10个工作日内进厂开展工作。

# 6. 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。

# 7. 质量保证

卖方在项目方案设计、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，出具的相关报告应得到行业/电力主管单位认定。

# 8. 保密要求

卖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，互相承担保密责任。

# 9.考核细则

9.1 遵守发包方有关规章制度，如违反则按发包方相关制度考核。

9.2 施工时应严格按检修工艺流程进行，如违反，发现一次扣款500元。

9.3 开工后现场项目经理、主要管理人员必须每天在施工现场，有事外出须向发包方请假，并另指定他人代为负责。否则，每人/次收取罚金500元。

9.4 施工所用人员、机械必须保证满足发包方项目的安全、质量、进度要求。如不能达到以上要求，发包方有权更换施工队伍并另行委托，其一切费用由施工方承担。

9.5 施工中每道工序完成后均需要由发包方验收合格后方能进行下一道工序。若未经验收进行下一道工序除返工外，则罚扣人民币1000元/次。

9.6 因项目质量问题进行返工所产生的一切费用均由承包方承担。

9.7 项目整体验收时，每发现一条缺陷扣款500元。

9.8 工期要求：承包方必须在协议工期内完成，每推迟一天扣项目款5000元。

9.9 违反GB26860《电业安全工作规程》及福海创相关的安全管理规定，发现一次扣款500元，发现3次，停工整顿并扣合同款5%。

# 10. 违约解除条款

承包商方有下列情形之一，发包人可终止或解除本合同：

10.1 承包商技术服务人员、机具设备不足，发包方认为不能依合同完工时。

10.2 承包商违反本合同条款规定或发生事故不能履行合约。

10.3 承包商人员有偷窃、破坏发包方财产等违章、违法行为时。

10.4 承包商有其他违反约定的行为3次以上。

10.5 承包商提供的设备、材料严重不符约定标准，经两次纠正仍达不到标准时。

10.6 承包商不执行合同约定的义务。

10.7 承包商未能按时提供优质服务，给发包方或者第三方遭受人身、设备经济损失的。

10.8 承包商违反福海创相关管理规定。

承包商若因上述原因被终止或解除合约时，在福海创书面通知中止合同后，承包商必须无条件配合交接，否则造成的一切损失由承包商承担。

# 11. 技术文件交付

11.1承包商须在办理项目交接验收后4周内，按相关规范要求编制所有报告。

11.2交工文件数量：纸介质原件三份，电子可编辑光盘/U盘一份。以上所有纸介质文件均需组装成册，以精装版交付。