## 一、技术要求

# （一）项目依据及重要性

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于2016 年11 月7 日通过，于2017年6月1日正式实施了，第二十一条国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务”。对拒不履行网络安全保护义务的，由有关主管部门责令改正，给予警告;拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

# （二）实施内容

# 1、技术依据：

《关于加强省级重要信息系统安全保障工作的通知》（赣公字[2015]55号）

关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知（中办[2003]27号文件）

关于印发《信息安全等级保护工作的实施意见》的通知（公通字[2004]66号文件）

关于印发《信息安全等级保护管理办法》的通知（公通字[2007]43号文件）

关于印发《关于开展全国重要信息系统安全等级保护定级工作》的通知（公信安[2007]861号文件）

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《中华人民共和国网络安全法》(主席令53号)  
《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)  
《计算机信息系统安全保护等级划分准则》（GB/T17859-1999）  
《网络安全等级保护实施指南》（GB/T25058-2019）  
《网络安全等级保护定级指南》（GAT1389-2017）  
《信息安全等级保护管理办法》（公通字[2007]43号）  
《网络安全等级保护基本要求》（GB/T22239-2019）  
《网络安全等级保护安全设计技术要求》（GB/T25070-2019）  
《网络安全等级保护测评要求》（GB/T28448-2019）  
《网络安全等级保护测评过程指南》（GB/T28449-2018）  
《信息安全风险评估规范》（GB/T20984-2007）等

《信息系统安全安全管理要求》（GB/T 20269）

《信息系统安全工程管理要求》（GB/T 20282）

# 2、项目内容：

| **序号** | **服务名称** | **服务内容** | **备注** |
| --- | --- | --- | --- |
|  | 等保定级备案 | 信息系统完成等级保护定级和公安备案工作。 | 2个三级系统 |
|  | 等级保护测评 | 针对的安全状况，按照相应的测评标准，从技术和管理两方面对系统进行合规性验证，查找安全短板。 |
|  | 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。 |
|  | 网络安全重保服务 | 在重要保障时刻，通过在互联网出入口部署攻击阻断防护系统协助甲方完成突发网络安全事件工作。 |  |

以等级保护标准要求为依据，对江铃汽车集团财务有限公司系统在物理安全、主机安全、应用安全、网络安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理和系统运维管理10个层面实施等级测评，明确安全责任，了解安全保护现状，排查安全隐患，明确安全需求，并为确立安全策略、制定安全规划、开展安全建设整改工作提供参考，具体目标如下：

**（1）信息系统等级保护测评**

聘请第三方测评机构展等级保护测评检测。具体要求：工作阶段、流程、内容、及成果交付严格遵循《信息安全技术信息系统安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术 信息系统安全等级保护测评过程指南》（GB/T 22240-2020）文件，根据系统等级开展相应级别的单项测评和整体测评，并使用自主开发的等级保护智能评估系统提高测评质量并规避实施风险。测评报告内容及格式严格遵照《信息系统安全等级测评报告模版（2019年版）》。

按照《信息安全等级保护管理办法》、《信息系统安全保护等级实施指南》，遵循《信息安全等级保护基本要求》（GB/T 22239-2019）等技术标准，从每个信息系统的物理安全、网络安全、主机安全、应用安全、数据和备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等10个层面进行测评，为保障测评质量技术团队必须具备两名以上高级等级保护测评师参与本次项目，测评期间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，否则做无效响应。

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2份（加盖服务机构公章）。

**（2）安全建设整改方案设计及防护修复建议**

聘请第三方测评机构依据《信息安全等级保护管理办法》、《信息系统安全保护等级实施指南》文件要求，应按照等级保护第三级要求进行保护，依据《信息系统安全保护等级实施指南》，遵循《信息安全等级保护基本要求》（GB/T 22239-2019）对江铃财务公司2个三级系统进行建设整改分析，比较信息系统与国家标准要求之间的差距。

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》，严格遵循《信息安全等级保护安全建设整改工作指南》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问题；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）：《安全建设整改方案》。

**（3）网络安全重保服务**

具体要求：在重要保障时刻，通过在互联网出入口部署攻击阻断防护系统，依托网防 G01 、网探 D01、 腾讯、 360、奇安信、华为第三方互联网公司汇集的实时威胁情报数据，通过数据汇集、实时联动、攻击画像、情报共享，对监测到的恶意攻击源进行自动化阻断，拦截“敌在侦我”的正向网络攻击，阻断“敌已控我”的外联攻击。**（响应文件中需提供防护系统截图界面并加盖公章）。**

1. **质量保证**

服务响应时间要求：自接到应急响应通知后，1小时内到达采购人处。

服务内容：服务期内，成交供应商根据采购人实际情况，负责对交付成果中的文档进行免费修正、优化、补充和完善；服务期内，成交供应商负责有对本项目设计的信息系统提供免费的技术支持的义务，包括应急响应等技术支持服务。应急服务人员需具备专业应急技术服务能力。

1. **技术服务团队**

供应商须针对本项目拟派不少于5人的技术服务团队。

**注：以上“技术要求”为实质性要求，必须完全满足，否则响应无效。**