

附件

甘肃省武威市中级人民法院三级等保测评服务项目

采购技术规范书

1. 项目概述

1.1 项目背景

2017年6月1日实施的《中华人民共和国网络安全法》第二十一条、第三十八条明确要求实行网络安全等级保护制度，关键信息基础设施的运营者应当自行或委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估。

为了进一步提高甘肃省武威市中级人民法院信息系统的安全保障能力，根据国家及各部委、各行业主管单位相关要求对其重要信息系统进行信息安全等级保护测评及相关安全服务。现拟邀请具有相应资质的信息安全等级保护测评机构依据《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》（以下简称“等保 2.0”）等管理规范和技术标准，检测评估甘肃省武威市中级人民法院三级信息系统安全等级保护状况是否达到相应等级基本要求，并出具相应的《信息安全等级保护测评报告》。

1.2 项目目标

通过等级保护测评工作发现信息系统在网络安全方面的不足之处，找出甘肃省武威市中级人民法院三级信息系统与国家及行业等级保护标准要求之间的差距，可以有效地提高甘肃省武威市中级人民法院网络安全建设的整体水平，并且指明方向，有利于在信息化建设过程中同步建设网络安全设施，保障网络安全与信息化建设相协调；有利于加强对涉及国家安全、经济秩序、社会稳定和公共利益的信息系统的安全保护和管理监督；有利于明确国家、法人和其他组织、公民的安全责任，强化政府监管职能，共同落实各项安全建设和安全管理措施。为信息系统的安全提供合理化建议，并协助甘肃省武威市中级人民法院设计详细和合理的等级保护整改方案，通过安全建设整改工作能够使各信息系统达到相应安全保护等级的能力要求。

1.3 项目内容及范围

本项目对甘肃省武威市中级人民法院一个三级“数字法庭业务应用系统”开展等级保护测评服务，明确系统的等级保护符合程度，提高甘肃省武威市中级人民法院重要信息系统的整体安全水平和防护能力。

具体工作内容如下：

- (1) 对信息系统中的核心业务系统进行等级保护测评；
- (2) 根据测评结果输出等级保护测评报告；
- (3) 根据测评结果，进行系统科学的分析，提出整改建设，输出整改建议；

2. 安全服务

2.1 等保测评服务

2.1.1 测评标准

2.1.1.1 国家安全政策

《中华人民共和国网络安全法》

《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）

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《信息安全等级保护备案实施细则（公信安[2007]1360 号）》

《关于开展信息安全等级保护安全建设整改工作的指导意见（公信安[2009]1429 号）》

2.1.1.2 国家安全技术标准

《信息保障技术框架》（IATF）

《计算机信息系统安全保护等级划分准则》（GB17859-1999）

《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 信息系统安全等级保护定级指南》（GB/T22240—2008）

《信息安全技术 信息系统安全管理要求》（GB/T20269-2006）

《信息安全技术 信息系统通用安全技术要求》（GB/T20271-2006）

《信息安全技术 信息系统安全工程管理要求》（GB/T20282-2006）
《信息安全技术 信息系统安全等级保护实施指南》（信安字[2007]10 号）
《信息安全技术 信息系统安全等级保护测评要求》（报批稿）
《信息安全技术 信息系统安全等级保护测评过程指南》（报批稿）
《信息安全技术 网络基础安全技术要求》（GB/T20270-2006）
《信息安全技术 操作系统安全技术要求》（GB/T20272-2006）
《信息安全技术 数据库管理系统安全技术要求》（GB/T20273-2006）
《信息安全技术 服务器技术要求》（GA/T671-2006）
《信息安全技术 终端计算机系统安全等级技术要求》（GA/T672-2006）

2.1.2 测评内容

等级测评的现场实施过程由单元测试和整体测评两部分构成。

对应《基本要求》各安全控制点的测评称为单元测试，具体可分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、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十项测试任务。

整体测评是在单元测试的基础上，通过进一步的分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。

测评的内容包括但不限于以下内容：

a) 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；

b) 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。

1.1 安全物理环境

根据甘肃省武威市中级人民法院信息系统机房和现场安全测评记录，针对机房和现场在“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”以及“电磁防护”等物理安全方面所采取的措施进行，判断出与其相对应的各测评项的测评结果。

1.2 安全通信网络

根据甘肃省武威市中级人民法院信息系统安全通信网络测评记录,针对网络方面在“网络架构”、“通信传输”、“可信验证”等安全通信网络方面所采取的措施进行检查,判断出与其相对应的各测评项的测评结果。

1.3 安全区域边界

安全区域边界现场测评包括对甘肃省武威市中级人民法院信息系统网络边界的测评,测评内容包括“边界防护”、“访问控制”、“入侵防范”、“恶意代码防范”、“安全审计”以及“可信验证”。

1.4 安全计算环境

安全计算环境现场测评包括对甘肃省武威市中级人民法院信息系统中网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其它设备的测评,测评内容包括“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”、“数据备份恢复”、“剩余信息保护”以及“个人信息保护”方面。

1.5 安全管理中心

甘肃省武威市中级人民法院信息系统安全管理中心现场测评包括“系统管理”、“审计管理”两个方面的测评。

1.6 安全管理制度

根据现场安全测评记录,针对甘肃省武威市中级人民法院信息系统在安全管理制度方面的“安全策略”、“管理制度”、“制定和发布”以及“评审和修订”等测评指标,判断出与其相对应的各测评项的测评结果。

1.7 安全管理机构

根据现场安全测评记录,针对甘肃省武威市中级人民法院信息系统在安全管理机构方面的“岗位设置”、“人员配备”、“授权和审批”、“沟通和合作”以及“审核和检查”等测评指标,判断出与其相对应的各测评项的测评结果。

1.8 安全管理人员

根据现场安全测评记录,针对甘肃省武威市中级人民法院信息系统在安全管理人员方面的“人员录用”、“人员离岗”、“安全意识教育和培训”以及“外部人员访问管理”等测评指标,判断出与其相对应的各测评项的测评结果。

1.9 安全建设管理

根据现场安全测评记录,针对甘肃省武威市中级人民法院信息系统在安全建设管理方面的“定级和备案”、“安全方案设计”、“产品采购和使用”、“自行软件开发”、“外包软件开发”、“工程实施”、“系统交付”、“等级测评”以及“服务供应商选择”等测评指标,判断出与其相对应的各测评项的测评结果。

1.10 安全运维管理

根据现场安全测评记录,针对甘肃省武威市中级人民法院信息系统在安全运维管理方面的“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”以及“外包运维管理”等测评指标,判断出与其相对应的各测评项的测评结果。

2.1.3 测评交付物

项目实施完成后,测评技术服务方须提供以下交付物:

信息系统等级保护测评报告:

《甘肃省武威市中级人民法院信息系统安全等级保护测评报告》

附属材料:

《甘肃省武威市中级人民法院信息系统等级保护整改建议方案》

《甘肃省武威市中级人民法院信息系统等保测评项目过程文档汇编》