**上海高院信息系统等级保护测评项目**

根据上海法院信息系统的实际情况，参照《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）及国家有关政策标准，按照等级保护要求，制定合理的测评方案，在保证测评质量的前提下，完成**上海法院政务外网业务网骨干网、上海高院互联网5大应用系统（上海市高级人民法院门户网站、上海移动微法院—诉讼服务网子系统、上海移动微法院—12368诉讼服务智能子平台、上海移动微法院—法官工作移动端子平台、上海移动微法院—法官工作PC端子平台）、上海高院政务外网5大应用系统（审判管理系统、执行管理系统、司法管理系统、诉讼服务系统、保障系统）**的三级等级保护测评工作。

(1)测评内容要求

1）安全物理环境

安全物理环境评估将通过访谈、文档审查和实地察看的方式评估信息系统的安全物理环境保障情况。主要涉及机房。

2）安全通信网络

安全通信网络评估将通过访谈、检查和测试的方式评估信息系统的安全通信网络保障情况。主要涉及对象为：主要涉及网络互联设备与安全设备。

3）安全区域边界

安全区域边界评估将通过访谈、检查和测试的方式评估信息系统的安全区域边界安全保障情况。主要涉及对象为：主要涉及网络互联设备与安全设备。

4）安全计算环境

安全计算环境评估将通过访谈、检查和测试的方式评估信息系统的主机和应用安全保障情况。主要涉及主机（存储操作系统）和数据库管理系统、应用系统。

5）安全管理中心

安全管理中心评估将通过访谈、检查和测试的方式评估信息系统的各类安全管理情况。主要涉及对象为：应用系统鉴别数据、业务数据等系统关键数据。

6）安全管理制度

安全管理制度评估将通过访谈和检查的方式评估信息系统的安全管理制度建立情况。主要涉及对象为：信息安全管理体系、日常安全管理制度、重要操作规程及相关执行记录等。

7）安全管理机构

安全管理机构评估将通过访谈和检查的方式评估信息系统的安全管理机构建立情况。主要涉及对象为：安全管理机构设立文档、信息安全小组名单、岗位说明书、等文档及执行记录。

8）安全管理人员

安全管理人员评估将通过访谈和检查的方式评估信息系统的安全管理人员方面情况。主要涉及对象为：人事管理制度、外部人员访问要求等安全管理制度及执行记录。

9）安全建设管理

安全建设管理评估将通过访谈和检查的方式评估信息系统的安全建设管理方面情况。主要涉及对象为：系统建设过程中涉及的相关文档，如：系统定级报告、安全设计方案、测试验收报告等文档及软件开发、工程实施等方面的安全管理制度及执行记录。

10）安全运维管理

安全运维管理评估将通过访谈和检查的方式评估信息系统的安全运维管理方面情况。主要涉及对象为：系统运维过程中涉及的安全管理制度及执行记录。

（2）测评服务要求

1）服务商应严格按照信息系统相应的等级保护要求开展测评工作，并提交下述完整的文档资料：

●提交完整的测评方案及测评计划；

●提交测评中产生的测评问题汇总表等，并给出整改建议；待整改完成后，再对整改情况进行复核；

●测评工作完成后应出具相对应的安全等级测评报告。

2）服务商需承诺：

●具有独立法人资格及相应经营范围；

●投标人具备网络安全服务认证证书等级保护测评服务认证；

●项目负责人具有高级专业技术职称证书、CISP资质证书的优先考虑；

●在测评服务中所提供的测评服务团队人员（不包含项目负责人）数量不少于6人（其中驻场不少于2人）；具有CISP资质证书的优先考虑。

●需进行保密承诺，不得向任何第三方披露，不得将项目中资料用于约定事项以外的其他用途。

3）其他：

●投标人具有中国合格评定国家认可委员会检验机构（CNAS）证书、ISO 27001信息安全管理体系证书、CCRC信息安全服务资质认证证书（分项类别——信息安全风险评估服务资质）的优先考虑；

●投标人具有近三年以来等保安全测评服务项目业绩的优先考虑。