
上海市高级人民法院

信息系统等级保护测评项目

招标需求

一、项目概述

上海法院经过多年信息化系统建设，已经逐渐形成了一个成规模、有体系的软、硬件结合的综合信息化系统。面对众多的法院应用系统，通过有效的方式保障应用系统安全稳定运行是法院重要的基础工作，本次招标项目服务范围是上海法院互联网和政务外网信息系统，服务内容包括对上海法院互联网和政务外网信息系统的安全服务采购。

二、系统现状

上海法院互联网信息系统包含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，共五个系统。

上海法院政务外网信息系统包含上海法院政务外网业务网骨干网网络系统、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，共六个系统。

通过为上述信息系统提供安全服务，保障法院应用系统安全稳定运行。

三、服务地点

本项目服务的地点包括：上海市高级人民法院（肇嘉浜路 308 号，柳州路 393 号，东兰路 248 号，闵行区旗忠村光华路 2888 号）。

四、服务内容

本项目服务内容主要为安全服务采购，通过采购安全服务为上海法院

现有信息系统的安全提供保障。本次采购的安全服务包括：

互联网三级等保安全测评服务：对上海法院互联网五个系统（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）按照三级标准进行等级保护测评工作。

上海法院政务外网业务网（骨干网）等级保护测评服务：对上海法院政务外网业务网（骨干网）按照三级标准进行等级保护测评工作。

政务外网应用等级保护安全测评服务：对上海法院政务外网五个系统（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）按照三级标准进行等级保护测评工作。

五、安全服务采购内容及要求

（一）安全服务采购清单

序号	服务名称	服务频次
1	互联网三级等保安全测评服务	1 次
2	上海法院政务外网业务网（骨干网）等级保护测评服务	1 次
3	政务外网应用等级保护安全测评服务	1 次

（二）安全服务采购要求

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) 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) 人员要求：

中标方应充分理解本项目的技术及实施复杂度，组建技术服务团队，

参与本项目的各类人员应具备相应的技术能力。在服务期内，中标方不得随意更换项目组技术人员，若因特殊情况需要更换服务人员时，需经招标方同意后，方可更换技术能力、资格条件相同或更高的技术人员。

中标方需提供项目组人员名单（包括项目组织架构、人员职责、人员分工、职业资格等）。

3) 服务商需承诺:

- 具有独立法人资格及相应经营范围;
- 测评人员具备网络安全等级测评与检测评估机构服务认证证书;
- 在本测评服务过程中所提供的测评服务团队人员数量不少于6人(其中驻场不少于2人);
- 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;
- 投标人具备CCRC信息安全服务资质认证证书且方向为信息安全风险评估的为优。项目负责人具有硕士及以上学位、具备计算机与信息技术应用专业高级工程师及以上职称证书为优。