**等级保护测评服务项目**

**附件一 报名材料：**

**（注：以下附件1至附件3为实质性条款，没有对此作出完全响应的供应商将被拒绝）**

|  |
| --- |
| **报名信息** |
| 单位名称 | 联系人 | 联系电话（手机号） | 地址 | 邮箱 |
|  |  |  |  |  |
| **注：请报名供应商填写以上信息。** |

附件1 有效的营业执照或法人证书等证明文件，以自然人身份参与的提交自然人的有效身份证明

附件2 法定代表人/负责人身份证明

附件3法定代表人/负责人授权书

**报名材料格式：**

附件 1 有效的营业执照或法人证书等证明文件（复印件，须加盖供应商公章），以自然人身份参与的提交自然人的有效身份证明（复印件）

## 附件 2 法定代表人/负责人身份证明(格式，原件)

**法定代表人/负责人身份证明**

供应商名称：

单位性质：

成立时间： 年 月 日

姓名： 性别： 年龄： 职务：

系 （供应商名称） 的法定代表人/负责人。

特此证明。

附：法定代表人/负责人的身份证明：有效的身份证正反面复印件，或有效的护照复印件。

供应商名称（盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 附件 3 法定代表人/负责人授权书（格式，原件）

**（非法定代表人/负责人签署报名材料的，应提交法定代表人/负责人授权书及其附件；若报名材料由法定代表人/负责人本人签署，则可不用提交。）**

**法定代表人/负责人授权书**

 本授权书声明：注册于 （国家或地区的名称） 的 （公司名称） 的在下面签字或盖章的 （法定代表人/负责人姓名） 代表本公司授权 （公司名称） 的在下面签字或盖章的 （被授权人的姓名） 为本公司的合法代理人，就\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_的比选，以本公司名义处理一切与之有关的事务。

本授权书于\_\_\_\_\_\_\_\_\_\_年\_\_\_\_\_月\_\_\_\_\_\_日生效，特此声明。

法定代表人/负责人签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

被授权人签字或盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

公司盖章：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

附：

被授权人姓名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

职　　　　务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

电　　　　话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

被授权人的身份证明：有效的身份证正反面复印件，或有效的护照复印件。

**附件二 采购需求：**

1. **项目背景**

按照《中华人民共和国网络安全法》《信息安全技术网络安全等级保护》等法律法规要求，为保障北京市重点站区管理委员会信息系统网络安全，开展信息化系统网络安全等级保护测评工作。通过等保测评工作使北京市重点站区管理委员会信息系统满足国家法律法规及行业监管要求。及时发现信息系统内部的安全隐患与不足之处，提升系统的安全防护能力，降低被攻击的风险。

1. **项目依据**
2. 《中华人民共和国网络安全法》；
3. 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
4. 公安部、国家保密局、国际密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004] 66号）；
5. 《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）；
6. 公安部、国家保密局、国家密码管理局、国务院信息化工作办公室制定的《信息安全等级保护管理办法》（公通字 [2007] 43号）；
7. 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）。
8. 《信息安全技术 网络安全等级保护定级指南》（GAT1389-2017）
9. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
10. 《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）
11. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）
12. 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）
13. 《信息安全技术 关键信息基础设施安全控制指南》（征求意见稿）
14. 《信息安全技术 关键信息基础设施网络安全保护基本要求》（征求意见稿）
15. 《信息安全技术 个人信息安全规范》（GB/T 35273-2017）
16. 《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）
17. 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）
18. 《关键信息基础设施安全保护条例》（征求意见稿）
19. 《网络安全等级保护条例》（征求意见稿）
20. 《网络关键设备和网络安全专用产品目录（第一批）》
21. ISO/IEC17799:2005/27001
22. IATF《信息保障技术框架》
23. **服务目标**

要对5个二级信息系统（北京市重点站区管理委员会网站，内控系统，档案管理系统，重点站区视频监控系统，交通数据处理平台）开展等级保护测评工作。

根据《信息安全技术-网络安全等级保护基本要求》GB/T22239-2019，结合北京市重点站区管委会的业务情况和行业要求，从安全物理环境、安全区域边界、安全通信网络、安全计算环境、安全管理中心等方面对系统的主机、应用、数据库、运维终端等进行等级保护测评。

1. **服务方式**

采取现场与远程相结合的方式进行测评。

1. **服务频率**

本项服务在一年服务期内，开展1次。

1. **服务范围**

北京市重点站区管理委员会网站，内控系统，档案管理系统，重点站区视频监控系统，交通数据处理平台5个信息系统。

1. **服务成果**

在本项服务完成时，将提交（但不限于）如下文档：

《信息安全等级保护测评报告》。

**八、资质要求**

供应商可提供ISO9001质量管理体系认证证书，业务范围需包含网络安全等级保护测评；

供应商可提供ISO27001信息安全管理体系认证证书，且业务范围包含网络安全等级保护测评；

供应商可提供由中国网络安全审查技术与认证中心颁发的信息安全风险评估服务资质一级证书；

供应商可提供由中国网络安全审查技术与认证中心颁发的信息安全应急处理服务资质一级证书；

供应商可提供由中国信息安全测评中心颁发的信息安全服务资质证书。