1 项目背景

北京市科学技术协会是北京地区科技工作者的重要组织，承担着促进科学技术发展、科学普及、维护科技工作者权益以及推动国际合作与交流等多项职责。随着信息化技术的快速发展和广泛应用，我单位的各项业务已经全面迁移至政务云平台。为了进一步落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规要求，强化数据安全与隐私保护，整体提升安全防护水平，我单位拟引入第三方专业服务机构，共同推进 2026 年度的网络安全建设工作，确保关键业务的稳定性运行，防止因安全事件导致的业务中断。

2 服务内容及要求 a

市科协所属业务系统及数据均已部署在市政务云平台上，并采购了云服务商的部分安全服务。本项目所采购的第三方专业服务机构提供的安全运营服务与市政务云提供的安全服务是“互补不替代”关系。由政务云提供的普适化安全服务，本项目不再重复购买，比如主机加固、主机杀毒等；政务云不能提供的深度定制化服务是本项目的服务重点，例如在安全漏洞扫描、安全配置评估等服务中，需要更深入的技术支持和定制化的安全建议、对漏洞产生的深度分析、定制化风险评估模型、个性化防护策略设计、专项技术咨询服务等。在服务过程中要体现出专业深度、经验积累；能够提供定制化服务、贴合科协业务的服务计划；同时要和政务云平台密切合作，信息共享；能够为市科协业务和数据安全提供前瞻性和创新性的一揽子解决方案。具体要求如下：

2.1 服务期限

服务周期：自合同签订之日起 1 年。

2.2 服务地点

服务地点：甲方指定地点。

2.3服务要求

2.3.1 互联网资产核查服务

1.提供全年 7*24h 互联网资产核查服务，包括但不限于：资产测绘及变化监控、资产暴露面监测、敏感数据泄露监测、边界脆弱性监测(含漏洞、弱口令检

测)等。按月度、季度和年度输出《互联网资产核查服务报告》。

#2.支持识别各类互联网资产【需提供工具界面截图，证明支持识别上述资产类型】。

2.3.2 安全漏洞扫描服务

1.采用专业漏洞扫描工具针对互联网层面对北京市科学技术协会开展每年不少于 4 次（每季度至少一次、重要保障期前、新系统变更或上线前）的常态化安全扫描，发现应用、主机、系统、网页等层面在互联网攻击视角存在的安全隐患及风险，通过专业技术分析，协助完成问题整改修复，形成并提交《漏洞扫描及整改修复情况报告》。

#2. 服务工具需支持检测的漏洞数大于 390000 条，兼容主流标准，并提供国家信息安全漏洞库(CNNVD)兼容性资质证书。

#3.服务工具需支持扫描国产操作系统、应用及软件的安全漏洞，如华为欧拉、open 欧拉、统信、麒麟、bclinux、达梦、南大通用、人大金仓、神通、金蝶、东方通等，要求能够扫描大于 100000 条相关漏洞。

2.3.3 安全配置评估服务

1.使用自动化工具和人工相结合方式,开展每年不少于 4 次的安全配置评估服务，对系统中网络设备、操作系统、数据库、应用服务器等的配置进行安全检查，并提供《安全配置评估及整改建议报告》。

2.3.4 渗透测试服务

1.通过人工黑盒的测试方式,提供每年不少于 2 次非破坏性的常态化渗透测试，发现网络和业务系统中存在的安全缺陷，形成并提交《渗透测试及整改修复情况报告》。

2.3.5 安全加固支持服务

1.针对漏洞扫描、安全配置评估等服务中发现的安全漏洞和配置缺陷，提供加固意见和方案，并配合相关开发厂商或运维人员完成系统加固。

2.3.6 数据安全评估服务

1.提供每年不少于 1 次数据安全评估服务。根据行业特征、监管动向等选取合适的法律法规或标准作为评估依据，通过专业评估 过程识别发现单位数据安全和隐私风险，并输出《数据安全评估报告》。

2.3.7 安全运营服务

1.提供 7*24h 的远程威胁监测与响应，形成从监测、研判、预警、处置到优化的完整闭环服务。并按月度、季度和年度输出《安全运营服务报告》。

2.每周针对攻击检测规则及能力进行升级更新。紧急高危事件情况下，1 小时内提供自定义检测规则，24 小时内进行工具规则更新【需提供承诺书并加盖公章】。

2.3.8 应急响应服务

1.提供 7*24h 应急响应服务，协助安全事件应急处置、分析研判。快速响应各类安全事件或疑似安全攻击行为，协助排查分析、确认影响范围，提供加固整改建议，及时抑制和消除信息系统网络安全事件，减少因网络安全事件而引起的损失和负面影响。根据实际情况提交《应急响应报告》。

2.3.9 应急演练服务

1.根据实际情况，每年至少组织 1 次应急演练活动，全面检测防守措施的有效性和弱点，以及在遇到突发情况下的应急措施和应急机制的有效性。应在事前制定详细周密的应急演练方案，在事后进行评估总结，做好安全措施的优化和改进指导，形成并提交《应急演练报告》。

2.3.10 重要时期保障服务

1.在重要活动、重要会议、重要节假日等重点保障时期进行保障，建立防护、监测、响应等安全运行机制，主动做好网络安全应急响应准备，保障关键信息基础设施和重要信息系统在重大活动期间安全稳定运行，避免出现安全风险事件。形成并提交《重要时期保障报告》。

2.3.11 网站云防护服务

1.提供不少于 20Mbps 防护带宽，包含不少于 5 个二级子域名的网站云防护。可防护 web 攻击/cc 攻击、网页防篡改等，并提供远程技术支持及专家服务。

2.支持站点接入，包括 HTTP、HTTPS 协议，支持 80,8080,443,8443 等标准端口。同时开放任意非标 WEB 端口配置途径，不作限制。【需提供工具界面截图，证明支持 HTTP、HTTPS 协议的非标 WEB 端口】

2.3.12 网站安全监测服务

1.提供 7*24h 远程网站安全事件值守服务，包含站点的 DNS 解析监测、挂马、黑链、篡改、敏感内容等监测，并提供每月一次漏洞扫描及验证服务。

2.3.13 安全情报通告服务

1.通过各种途径实时关注、收集相关安全威胁情报，搜集和整理漏洞信息、系统补丁信息、病毒信息、行业重大安全事件等信息，提供高危漏洞通告、行业安全事件周报。

2.3.14 数据分类分级

1.采用自动化与人工相结合的方式，对北京市科学技术协会指定的数据资源明确数据分类分级指引、流程和对应措施；建立分类分级框架，确定分类分级规则并建立台账。

2.3.15 其他工具要求

1.本次招标中所需服务工具，必须为适用于虚拟化环境的版本。投标方所提供的服务工具应兼容政务云环境，能够无缝集成至现有云平台。

2.3.15.1 数据分类分级工具

序号	指标项	重要性	要求描述
1	性能		扫描速度≥80 字段/s
2	支持数据库	#	至少支持对 EnterpriseDB、IRIS、Oracle、MySQL、SQL Server、DB2、AS400、Informix、Sybase、Cache、PostgreSQL、MariaDB、MongoDB、SAP HANA、达梦、GBase 8a/8s、Kingbase、TDSQL PostgreSQL、GaussDB（A/T）、TDSQL MySQL、OceanBase、Inceptor、TiDB、GoldenDB、PolarDB-PostgreSQL、PolarDB-MySQL、StarRocks、RDS-PostgreSQL、PolarDB-Oracle、RDS-MySQL、MaxCompute、HashData、Cloudera Impala、Hive、Teradata、Elasticsearch、GreenPlum、ClickHouse 等数据库类型的分类分级。【需提供工具界面截图，证明支持上述所有数据库的审计】
3	数据源管理		文件支持通过 FTP 上传或本地上传，至少支持 txt、json、xml、excel、csv、del 等。
4		#	支持逐步新建数据库时，将数据库与所属机构、资产分组、用户组、应用类型、应用及元数据做关联，同时支持数据库的批量导入导出。【需提供工具界面截图，证明支持将这些数据做关联】
5	数据资产主动扫描	#	支持在分类分级模板中基于多个标签及表的行数设置表的分类分级策略。【需提供工具界面截图，证明支持基于标签与行数设置策略】

6		#	在表打标中支持显示表的行数及大小。【需提供工具界面截图，证明支持显示表的行数及大小】
7			支持打标主表后，将结果同步至表结构相同的表。
8		#	数据地图中需要展示资产的表总数、字段总数、打标总数、打标率、手动修正率等。【需提供工具界面截图，证明支持展示相关数据】
9			支持对分类分级的结果进行手动打标、批量打标、导入导出打标等。
10	服务期限	#	此工具服务期限为数据分类分级开始至结束，工具服务期限需完整包含项目服务期限。

2.3.15.2 数据库审计系统

序号	指标项	重要性	要求描述
1	性能		SQL 语句处理性能≥ 5000 条/s 数据库网络流量处理能力≥ 1000 Mbps 入库语句量≥3000 条/s
2	支持数据库	#	至少支持 Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、MariaDB、Cache、Teradata、Impala、Greeplum 等国际主流数据库审计。至少支持 DM、kingbase、OSCAR、Gbase、Highgo、Guass DB、TDSQL-MySQL、TDSQL-PostgreSQL、GoldenDB，TiDB，星环 inceptor 等国产数据库审计。【需提供工具界面截图，证明支持上述所有数据库的审计】
3	审计规则		支持对数据库访问行为建模，维度至少应包含：数据库对象、账号、客户端 IP、客户端工具以及操作类型。
4		#	支持利用访问行为模型建立审计基线，对超出基线模型的操作可自动识别和告警。【需提供工具界面截图，证明支持建立审计基线，对超出基线模型的操作可自动识别和告警】
5	SQL 注入检测		支持 SQL 注入检测，内置 SQL 注入特征库，可根据审计要求自定义 SQL 注入规则。
6	风险防御	#	支持镜像旁路部署下，对风险 IP、风险账号、风险工具、风险时间段、风险语句进行阻断，且支持自定义阻断时长。【需提供工具界面截图，证明支持旁路阻断功能】
7	IP 别名		支持 IP 别名建立，方便审计与风险跟踪。
8	告警与响应		支持根据行为操作、SQL 注入、漏洞攻击检测等风险告警定义，按照高、中、低风险级别与响应方式关联进行告警。
9	售后服	#	提供一年原厂售后服务承诺。

	务		

2.3.15.3 日志审计系统

序号	指标项	重要性	规格要求
1	性能		默认支持接入 50 个日志源，最大可扩展接入 100 个日志源；支持不低于每秒 2000EPS 的日志平均处理能力
2		#	系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统、Windows 共享文件审计等【需提供工具界面截图，证明支持上述所有数据采集范围】
3		#	系统支持采集国产化操作系统日志，包括但不限于：中标麒麟、银河麒麟、统信、凝思、华为欧拉、龙蜥、中科方德、中科红旗等【需提供工具界面截图，证明支持上述所有国产化操作系统的日志采集】
4			系统应支持规则自适应日志接入，仅输入 IP 范围及端口即可自动匹配相应规则，完成日志自动接入
5			系统应支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式
6		#	系统应内置对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联等。【需提供工具界面截图，证明支持针对主机进行上述的深入分析】
7		#	系统应内置对 WEB 服务器日志展开深度分析，分析内容包括但不限于发起请求的地址及浏览器情况、响应结果、访问趋势等。【需提供工具界面截图，证明支持针对 WEB 服务器日志进行上述的深入分析】
8			支持通过前置、后置两种不同方式自定义配置丢弃规则，将用户不关心的日志进行过滤
9	售后服务	#	提供一年原厂售后服务承诺。

3. 团队成员情况

为保障本项目中各项安全服务的有效实施与持续运营，投标人应承诺为本项目配备专职、稳定的服务团队，并提供详细的组织结构、人员简历、岗位职责及资质证明。团队应至少满足以下配置：供应商需为本项目成立专门的不少于5人的项

目团队，其中项目经理1人。

3.1 需要配置项目经理一人，负责安全服务项目支撑团队的总体协调与沟通工作；开展项目管理工作，确保本项目团队按照客户要求完成各项工作；负责遵守各项管理制度，健全和落实质量保证体系，保证成立的项目组织机构人员及相关资源投入的质量和数量，确保项目能够在规定的时间内高质量的完成。与项目领导组一起承担合同范围内的各项项目任务全面完成的重要职责，管理项目进度、范围、质量、风险等。

项目经理要求：应具备5年（含）以上网络安全项目管理经验，持有信息系统项目管理师（高级）、CISP证书，能组织团队成员优质高效完成本项目既定目标。

3.2需配置技术负责人一人，负责对项目技术规划与决策、技术方案执行与优化、应急响应与演练主导、沟通协调与技术支持。

项目技术负责人要求：应具备5年（含）以上网络安全技术经验，具备信息系统项目管理师（高级）证书。

3.3其他人员：

需配置技术团队，（除项目经理和技术负责人之外），包含技术方案设计，质量全程把控，服务实施，项目的网络安全和数据安全保障工作，对项目运行过程中的安全风险防控和安全事件处理负责。项目团队应确保能同时支撑常态化安全运营（7*24小时监测、资产核查）、周期性安全评估（漏洞扫描、渗透测试）及应急响应任务。

团队成员要求：应具备中国网络安全审查技术与认证中心颁发的信息安全保障人员认证证书-安全运维（专业级）、中国网络安全审查技术与认证中心颁发的信息安全保障人员认证证书-风险管理（专业级）、中国网络安全审查技术与认证中心颁发的信息安全保障人员认证证书-应急服务（专业级）证书。

供应商需具有较强的专业技术人员队伍和装备，深入了解并准确把握相关法律法规和技术标准，能快速响应采购人的需求，具备开展相关工作的能力和经验。供应商需保证按时提交成果。供应商对委托项目的内容、成果予以严格保密，未经采购人同意不能泄露给第三方，确保实施过程中不出现数据失泄密事件发生。

4.验收要求：

按招标文件采购需求以及投标文件响应情况逐项进行验收。