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。为更好地履行维护网络安全、意识形态安全和国家安全的使命，按照中央和北京市要求，北京市科学技术协会(以下简称“市科协”)需要全面加强“数字科协”大数据中心的安全运营保障工作，加强对部署在政务云上的平台主机安全防护，加强对数据汇聚接入中心、人工智能分析中心、数据共享中心、用户中心等平台系统和功能模块的管理，加强平台对与北京市大数据中心和其他相关单位平台的数据交换与敏感信息安全管理，全面提高市科协对“数字科协”大数据中心的安全保障及运维管理水平。

由于“数字科协”大数据中心需要对接北京市大数据中心平台和其他数据源，同时运维管理工作内容复杂，专业性要求高，故将通过第三方外包服务的方式，协助科协开展系统安全防护和数据安全防护以及数据备份等安全运营工作，确保“数字科协”大数据中心正常运行使用，相关业务顺利开展。

2.服务内容及要求

确保“数字科协”大数据中心能够稳定、安全、快捷的对内外提供服务，确保相关数据内容安全、准确、及时，满足安全等保三级要求。

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、漏洞扫描等；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。

2.1 服务期限

服务周期：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资产暴露面核查服务

1.利用技术手段对在网络环境中暴露的资产进行收集探测，帮助市科协发现未知资产、暴露面、信息泄露等情况。发现内容包括：1.域名资产；2.IP 资产；3、开放的端口服务；4.查找网络空间泄露的账户密码、应用数据敏感信息、内部资料、系统源代码、通讯录信息和网络拓扑信息等。按月度输出《资产暴露面核查服务报告》。

2.3.2安全漏洞扫描核验服务

1.采用人工深度验证方式，精准发现主机层，应用系统层 ，中间件层漏洞中存在的高危漏洞（如远程代码执行、权限绕过、数据泄露等）。通过专业技术分析，协助用户明确漏洞危害等级、影响范围及利用路径，并配合用户完成整改。

2.3.3 基线核查服务

1.使用人工方式对系统中网络设备、操作系统、数据库、应用服务器的配置进行核查，协助用户完成配置整改。采用人工深度验证方式，精准对网络安全设备、服务器操作系统、数据库、应用服务器等配置结果进行核查验证，并协助用户完成整改。

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、基线核查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，并提供漏洞扫描及验证服务。

2.3.8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】。

2.3.9安全情报通告

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。

2.3.10应急响应服务

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》。

2.3.11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》。

2.3.12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》。

2.3.13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。

2.3.13.1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	国际主流数据库		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。
3	国产化数据库	#	至少支持 DM、kingbase、OSCAR、Gbase、Highgo、GuassDB、TDSQL-MySQL、TDSQL-PostgreSQL、GoldenDB，TiDB，星环 inceptor 等国产数据库审计。
4	审计设置	#	支持数据库访问行为与返回结果集的双向审计，支持结果集支持最多保存行数与最大保存长度大小自定义。同时支持全量审计与满足审计规则审计模式切换。
5	协议栈支持		支持在 IPV4、IPV6 环境中部署，支持所有数据库 IPV4、IPV6 协议的审计，且支持 IPV4、IPV6 混合流量审计。
6	复杂语句审计	#	支持审计复杂 SQL 语句以及绑定变量的复杂 SQL 语句，操作层级≥5 级，≥30 行。
7	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。
8		#	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。
9	审计查询		支持审计内容的海量查询与审计数据导出，单次导出数据≥100 万条。
10	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。
11	配置管理		支持一键备份系统配置与一键清空配置。
12	系统告警		支持系统告警功能，点位设备异常类型以及当前状态。告警类型包括：异常关机、分区超限、压力超限。
13			支持系统资源监控与告警，支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，系统会发出告警。
14	补丁管理		系统软件包、补丁包需具备完整性校验能力，校验失败终止操作。

2.3.13.2日志审计系统

序号	指标项	优势	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	功能		系统应提供前端界面自定义能力，应支持用户自定义文字标题、主题色、LOGO、版权信息、技术支持电话、企业官网地址、界面二维码等多种元素
3		#	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

4		#	系统支持采集国产化操作系统日志
5			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
6			系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译
7			系统应支持基于 SM2、SM3、SM4 等国密算法对日志进行数字签名验签操作，以满足日志完整性校验要求
8		#	系统应能够对 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
9			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

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：具备5年（含）以上工作经验，持有信息系统项目管理师（高级）、CISP证书、CISAW证书。

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。

技术负责人要求：具备5年（含）以上工作经验，持有信息系统项目管理师（高级）证书、CISP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。

团队成员要求：不限于网络操作系统，网络安全，数据安全，网络系统，应

用安全，TCP/IP协议,OWASP TOP10风险，主流操作系统安全配置，熟练运用Nessus，Burp Suite，Wireshark等工具开展漏洞挖掘，渗透测试与安全加固掌，握应急响应全流程与日志分析技能，熟悉等保2.0等合规标准与相关法律法规等。团队人员具有CISP证书、信息安全工程师证书等。

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。