一、采购项目概况

为扎实落实《网络安全法》《数据安全法》《个人信息保护法》等法律法规要求，提升网络安全管理工作水平，做好重要时期重点信息基础设施网络安全保障，筑牢网络和数据安全防线，保障社会经济高质量发展，拟采购网络安全相关技术服务。一是能建立定期更新的网络安全基础数据资料库，摸清重点行业、重点单位底数，提高网络安全防范工作的预见性和有效性。二是能提供专业及时的技术服务，发生网络安全事件后准确研判危害等级，迅速制定处理方案，有效控制损失和危害范围。三是能为网络安全人员提供业务培训，定期组织实施网络安全应急演练，提高网络安全队伍的专业技术和业务能力。

二、服务要求

1.网络安全检查服务：在服务期内依据指定单位（服务期内检查数量不少于40家）进行网络安全专项检查工作，包括合规性检查和技术检查，并输出相关检查报告。

2.安全培训服务：在服务期开展网络安全人员网络安全培训。不少于3次/年，应提供培训场地、培训相关资料、培训讲师（应具备相关资质）等。

3.重要时期网络安全保障服务：提供重保安全服务，对重要信息系统（不少于10套）进行网络安全问题排查，并提供完善的建议，保证信息系统在重大活动期间的正常运行。不少于30人天/年。

4.网络安全制度体系建设服务：建立、完善适合用户需

求的网络安全管理制度体系，根据国家相关法律法规的变化及时对制度体系进行更新优化。提交经专家评审制度 1 套。

5.网络安全管理体系建设服务：建立、完善适合用户需求的网络安全管理制度体系、网络安全管理机构、具体工作职能部门和岗位、安全技术防范及相关安全类文档体系等;帮助用户制定各项管理政策、网络安全类相关制度、表单等，讨论解决安全管理中的重大问题；协助用户构建并完善网络安全管理体系。提交管理体系资料 1 套。

6.应急响应服务：采取有效的应对措施，控制安全事件造成的影响范围，缩小损失，排查问题来源，恢复网络和信息系统正常运行。应急支撑不少于 40 人天/年。

7.应急预案及演练服务：协助用户编制应急预案，然后通过应急演练检验本单位相关人员在应对网络安全突发事件的组织指挥和应急处理能力，分析演练中暴露的问题，不断修订完善应急预案，提升本单位的网络安全应急处置水平。提交经专家评审应急预案 1 份，并开展应急演练 1 次，提交应急演练报告 1 份。

8.互联网专项治理服务：互联网专项治理服务主要是根据上级部门要求，完成指定目录网站的筛查工作，标注仿冒钓鱼类备案异常类、内容异常类等类型。筛查数量不少于 5000 个/年，并满足上级工作要求。

9.网络安全风险通告服务：通过邮件、企业公众号或直接发送的方式向用户提供安全风险相关的安全通告、最新

重大网络安全事件通告(安全漏洞通告、媒体关注通告和恶意 IP 通告等)服务。风险通告不少于 50 条/年。

10. 开展为期一周的线上、线下宣贯活动，同时针对管理、技术人员开展培训活动。活动内容不少于 5 项。

11.网络安全资料库建立及更新服务：本服务整体交付资料，结合用户行业工作特点，整合本项目整体交付资料，包括管理类、制度类、检查类、风险类等全面资料，形成相关资料库。服务期结束时提交资料库 1 套。