项目需求

为有序配合网络安全攻防演练，做好防守工作，投标人应根据采购人要求编制服务方案。

投标人应投入充足的专业技术人员，且具有较强的后端服务支撑能力，能够及时响应服务期间采购人的紧急性、突发性服务支持需求。后端支撑团队服务支撑内容包括但不限于提供日常安全监测、疑难安全事件分析研判、安全情报分析、突发性事件处置，必要时能够通过后备人员及时补充服务力量。

投标人负责对参与重要环节的人员进行背景审查，投标人需与参与服务人员提前签署保密协议，不得泄漏目标单位任何信息。

**工作内容如下：**

**一、准备阶段**

1、制定保障工作整体方案及工作计划，输出防守保障方案；

2、开展安全意识培训，全面提升全员防范意识，避免被攻击队钓鱼攻击；

3、对单位内资产进行梳理，包括互联网资产梳理、内网资产梳理（服务器、网络、安全设备、业务系统）、外网开放服务梳理等，在已有梳理结果上进行补充完善；

4、开展各项安全风险排查工作（漏洞扫描、渗透测试、弱口令排查、敏感信息排查），全面评估我单位存在的网络安全隐患问题，以检查促防护，推动建立和完善核心重要系统网络安全防范体系。评估内容包括，对信息系统进行漏洞扫描，包括漏洞扫描及按需复检，发现系统环境潜在风险隐患，提供专业安全测评报告和提出整改建议；采用工具或人工方式对操作系统、数据库、网络设备、安全设备、应用程序等进行弱口令专项检查，跟踪和指导弱口令整改，做好复检；模拟黑客可能使用的攻击技术，通过本地或远程方式对目标系统的安全作深入的非破坏性探测，通过安全工具以及人工渗透测试，尝试入侵系统，发现系统各个层面存在的漏洞，对过程中发现的问题及风险提出安全加固建议；互联网网站、网盘、百度文库等涉及我单位敏感信息排查；

5、建立联防联控防守团队，明确防守流程，沟通防守机制，并制定常见安全事件入侵应急预案；

**二、安全加固与防护强化阶段**

1、协助完成安全漏洞整改，协助对准备阶段漏扫、渗透、弱口令排查发现的安全风险进行整改，并完成问题复核工作。

2、收紧互联网暴露面，协助老旧、废弃、存在高风险系统下线，减少攻击面暴露；协助收紧防火墙策略，关闭不必要对外映射服务；

3、安全防护能力提升，协助完成访问策略控制优化、防火墙策略优化、安全设备策略优化、主机加固等工作；

**三、正式演练防守阶段**

网络攻防演习期间，安排人员开展24小时现场实时安全监测、研判分析及应急处置等安全值守服务，指导网络值班员实时对态势感知系统及相关网络安全防护系统或安防设备的告警进行监视，组织并对期间出现的网络安全异常和告警进行快速处理，实时对抗攻击队伍，应对并成功处置网络攻击，确保各水利信息系统的网络安全稳定。每日对防守情况进行复盘总结，按照要求输出防守报告。

**四、项目总结阶段**

结合攻防演练成果及复盘结论，对我单位信息系统网络安全防护技术措施进行全面评估分析，并对所发现的安全威胁提供解决方案并协助优化，输出防守总结报告，并协助完成上级单位要求的安全漏洞整改及复核工作。