涉进博会红线内重点系统专项保障服务需求

一、项目背景

今年，由商务部、上海市人民政府主办，中国国际进口博览局、国家会展中心（上海）有限责任公司承办的第九届中国国际进口博览会（以下简称“进博会”）将国家会展中心（上海）举行。按照《第九届中国国际进口博览会城市服务保障总体方案》的部署要求，市委网信办会同市公安局，共同牵头开展进博会网络安全保卫工作，组织开展进博会安全安保社会面重点单位、要害部门、重要网络信息系统等网络安全专项检查，督促相关单位落实网络安全主体责任；加强网络安全协同防护，确保涉及进博会官方网站、线上办展、在线会议等涉博重要网络系统的安全、稳定运行。

二、服务需求

完成涉进博会红线内重点系统专项保障工作，主要工作内容包括以下方面：

（一）机房网络终端设备及系统应用安全检查

采取网络巡查和现场检查方式，对红线内2个机房、红线内

以及周边配套网络设备终端开展安全检查，对红线内核心系统开展僵木蠕毒查杀检查，提前发现安全风险，整改缺陷。

（二）红线内系统渗透测试

针对红线内重要信息系统和应用，开展远程漏洞扫描和渗透注入点探测，针对系统提权漏洞和渗透注入点进行扫描发现，快速发现红线内重要信息系统和应用的漏洞风险，防止攻击者通过漏洞植入后门、窃取核心数据、破坏服务器等，为之后漏洞修补、渗透注入点修复的整改工作提供支撑。

（三）进博会重要核心网站和系统攻防实战

采用国家网络攻防演练的攻防和沙盘平台，向上对接国家网络攻防演练库，向下复盘典型攻防场景，针对全市直接为进博会提供服务的重要网站和信息系统，特别是新增线上系统开展应用和系统攻防实战。

本项工作主要可利用的手段包括：Web 系统安全漏洞，例如注入漏洞、命令执行、文件上传等；通用中间件系统漏洞，例如反序列漏洞、弱口令等；业务逻辑漏洞，例如弱口令、水平越权、垂直越权等；利用人性的弱点进行攻击，例如常见的钓鱼邮件、OA 钓鱼、IM 钓鱼、水坑攻击等。

（四）红线内系统压力测试

对红线内核心网站和系统进行压力测试，对高并发访问进行仿真模拟验证，或使用出口云防设备对系统日常访问压力进行检测和监测，检验红线内系统承载能力及抵御大流量攻击的能力。

（五）红线内核心系统网站实时监测

针对红线内核心系统网站持续进行 7*24 安全监测，通过自动化平台支撑，及时发现网站应用漏洞问题的变化现状（应用存在不断迭代更新的现状），提高问题清零准确率和有效率。监控内容包括但不限于网页挂马监测、异常文件监测、网站暗链监测和网站漏洞监测等。

（六）线上会议专线安保技术服务

针对进博会开幕式、线上直播和线上会议视频连线等提供现场网络安全保护，包括会议全程值班驻守，现场巡查、检查、协调安保事务，对进博局相关系统以及线上直播会议中的所有突发网络安全事件进行研判、协调、处置等。

三、服务要求

1.为了保证项目的顺利实施，确保项目质量达到预期目标，中选单位应成立项目实施组，并明确各角色职责，利于加强项目管理和各方面协调合作，使工作和责任更加清晰明确;

2.中选单位应根据检查测试结果，向被检查单位提出整改建议，并保留原始检查记录表和扫描测试报告。

3.在服务实施期间，中选单位避免影响相关单位网站的正常运行，检测结果严格按照规定报送，不得擅自对外发布或提供给无关机构。

四、综合能力要求

1.供应商具有与本服务项目相关的平台或软件著作权或专利专有技术的，优先考虑。

2.项目组人员岗位配备合理，专业能力、投入时间应与需求相匹配。

投入本项目团队中项目负责人具有信息系统项目管理师（高级）证书、中国信息安全测评中心颁发的注册信息安全专业人员(CISP)证书、具有不少于 8 年网络或信息安全测评工作经验的为优。

项目团队不少于 20 人；团队中有不少于 5 人具有中国信息安全测评中心颁发的注册信息安全专业人员(CISP)证书的、具有等级保护测评师证书的，优先考虑。