宁东基地2023年网络安全实战攻防与对抗演习

比

选

文

件

编制单位：宁东管委会科技和信息化局

编制时间：2023年5月15日

宁东基地2023年网络安全实战攻防与对抗演习服务单位比选文件

为深入贯彻落实习近平总书记关于网络安全工作系列重要讲话精神，切实做好新时代宁东基地网络安全工作，有效应对复杂严峻的网络安全形势，精准提升宁东基地信息系统抗攻击、抗入侵的能力水平，按照《宁东能源化工基地管委会政府投资项目招标投标管理监督暂行办法》和《宁东能源化工基地管委会政府投资项目招标投标管理监督暂行办法的补充规定》的有关要求，通过比选的方式，确定宁东基地2023年网络安全实战功放与对抗演习。现将相关事宜公告如下：

一、项目概况

项目名称：宁东基地2023年网络安全实战攻防与对抗演习；

服务地点：宁东基地；

服务期限：自合同签订之日起至攻防演习完成；

服务内容：本项目负责宁东基地的网络安全实战攻防与对抗演习的方案编制、协助组织全流程网络安全实战攻防与对抗演习及加固指导服务等；

项目预算：预算金额50万元。

二、比选文件

**（一）提交比选文件应包括下列内容：**

1.报价函；

2.授权委托书；

3.参选人基本情况表（须附相关资质复印件并加盖公章）；

4.参选文件（演习方案、业绩等）

**（二）比选文件的份数和签署**

1.参选人提交比选文件，一式叁份。

2.比选文件均需打印或使用不褪色的蓝、黑墨水笔书写，字迹应清晰易于辨认。

3.比选文件中要求加盖参选人公章或要求法定代表人及其授权代表签字的地方均应盖章或签字。由授权代表签字或盖章的在比选文件中须同时提交比选文件签署授权委托书。比选文件签署授权委托书格式、签字、盖章及内容均应符合要求，否则比选文件签署授权委托书无效。

**（三）比选文件的装订、密封和标记**

1.比选文件应装订成册进行胶装，并编制目录，装订应牢固、不易拆散和换页。

2.比选文件必须密封递交，未密封的文件不予接受。对封装材料及样式不作特别规定，但参选人应当保证其封装的可靠性，不致因搬运、堆放等原因散开。

3.比选文件密封袋上均应注明名称、参选人名称并加盖参选人印章。

三、比选文件的提交

比选文件应在2023年5月19日9:40时前提交至宁东基地管委会4楼3号会议室，2023年5月19日9:40时之后不再接受比选文件。

四、比选

1.比选时间：2023年5月19日10:00时

2.比选地点：宁东管委会4楼3号会议室

3.参加人员：三名评审专家、科技和信息化局

4.比选程序：

（1）比选由科技和信息化局主持。

（2）由监督单位检查比选文件的密封情况。

（3）经确认无误后，由有关工作人员当众拆封，科技和信息化局对参选单位进行资质审查，专家评审小组评分，确认中选单位。

五、监督单位

比选监督单位由办公室、财政金融局担任。

六、项目服务要求

**（一）技术要求**

本项目负责宁东基地网络安全实战攻防与对抗演习的方案编制、协助组织全流程网络安全实战攻防与对抗演习及加固指导服务等。

**1.准备阶段**

（1）参演单位情况调研

方案编制前，完成对宁东基地企业实地调研，确定参演单位。主要针对企业资产范围、靶标系统、攻击方式等内容进行明，并对后续参演单位的防守方案提供技术指导。

（2）演习方案编制

在前期准备的基础上，完成《网络安全攻防演练工作方案》按照方案开展演练活动的各项准备工作。

（3）人员审核

在攻防演习开始前，应对参演人员尤其是攻击队成员进行人员审核、背景审查工作，确定参演人员无涉网违法犯罪记录，人员审核工作由指挥中心领导小组统一领导。

（4）演习授权及备案

演习开始前期，在对目标系统进行前期的安全准备工作中，参演单位应对第三方技术支撑单位进行正式授权。同时第三方技术支撑单位应向参演单位提供IP信息，参演单位将此次攻防演习工作情况及所使用的攻击IP地址等信息，向自治区网络安全相关主管部门（公安厅、网信办等）进行备案说明。确保演习各项工作，均在授权范围内有序进行。

（5）攻击方环境测试

攻击组测试网络环境、演习平台操作等相关测试。

**2.正式演习阶段**

（1）攻防演习启动会

演习全部人员参加，专家组宣布比赛规则，演习采用的攻击方式和风险规避措施及各工作小组职责及注意事项等。由主办方领导致辞，强调本次演习的意义、目的宣布演习活动正式开始。

（2）正式演习阶段

该阶段进入正式的演习环节，指挥中心领导小组对演练全过程进行指挥控制，掌握进展情况。各参与方需要按照演习方案进行应急演习，如有观摩的领导，可以增加现场解说。演习执行可以分为监测预警、事件研判、事件通告、事件处置以及系统确认五个阶段。演习实施过程中，评估人员按照演习方案采集评估素材。

（3）评估与总结阶段

分析演习记录及相关资料，对演习活动及组织过程进行客观评价，编写演习评估报告。根据演习记录、演习评估报告、演习方案等材料对演习进行总结，并形成演习总结报告，包括：演习目的、时间、地点、参演机构和人员、发现的问题和漏洞清单、经验和教训、改进措施和建议等。

（4）演习结束

闭幕阶段，由指挥中心领导小组成员宣布此次演习活动的成绩及成果总结，对参演单位量化评分排序，并对优秀攻击队伍和防守队伍进行表彰。

**3.成果利用及整改加固**

根据演习总结报告提出的问题和建议，进行安全整改和加固。对演练中发现的问题，持续改进，并及时修改和完善本单位信息安全应急预案。吸取经验，完善演习方案，并组织相关人员开展安全意识培训，制定下一步工作计划。

**4.规模和周期要求**

攻防演习采用红蓝对抗的形式，由最终中选单位组织5支及以上攻击队伍（每支队伍3人及以上）形成红方（攻击方）对宁东企业靶标系统发起网络攻击。由参演单位组织形成蓝方（防守方）在攻防过程中进行业务系统的实时状态监控、阻断、溯源等应急处置操作。

（1）演习周期为14个工作日（含启动会、复盘总结会）。

（2）中标方负责演练的方案、手册、秩序册、活动场地的布置、培训组织，配合甲方完成启动会、复盘总结会、培训等相关工作。

（3）红方队伍由乙方组建，参演成员须具备网络安全相关证书或参赛经验、严格审查参演人员资质、背景，并协助组建裁判组3人、专家组3人。

（4）本次演习使用的攻防演习支撑平台由第三方中选单位提供，攻击人员的所有行为通过平台进行记录、监管、分析、审计和追溯，保障整个攻击演习的过程可控、风险可控。同时，演练平台提供实况展示。

乙方要配备专职人员做好演练的准备活动、场地布置、展示宣传、启动会、正式演习、复盘总结会等全流程环节管控。

（5）系统平台需支持本地或其他部署方式，根据甲方需求开展。

**5.演习服务内容说明**

针对本次演习，乙方需提供攻防演练平台搭建、专家组、裁判组、攻击队伍、视频监控服务、演练宣传、会务保障、整改咨询、网络安全培训等服务。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **活动名称** | **活动内容** | **备注** |
| 1 | 演习平台搭建 | 提供攻防演习平台，可实现攻击实况展示等功能，提供流量审计设备租用，可对队伍操作进行溯源，保证全程可控； |  |
| 2 | 专家组 | 提供3名区内相关专家，对攻击演习全过程进行咨询； |  |
| 3 | 裁判组 | 提供3名网络安全专家，对攻防成果进行评判打分； |  |
| 4 | 攻击队伍 | 提供5支及以上具有网络安全赛事经验的攻击队伍组成本次演习攻击方，配备的团队成员在网络安全赛事中有获奖经验。 |  |
| 5 | 视频监控服务 | 提供视频监控设备和录屏软件，对演习期间所有攻击队员攻击行为和操作过程进行记录； |  |
| 6 | 演练宣传 | 演习期间制作各种宣传视频、展板、条幅等材料进行必要的宣传，对演习全过程进行拍照录像并制作不少于 5 分钟的宣传短片； |  |
| 7 | 会务保障 | 为参赛人员提供餐饮、住宿等后勤保障并提供1名应急处置专家，对攻防实战应急演习中发现的隐患进行或辅助应急处置； |  |
| 8 | 整改咨询 | 对攻防演习发现的问题清单，提供针对性的整改建议； |  |
| 9 | 网络安全培训 | 结合攻防演习的案例以及甲方需求，制作培训材料进行2次以内网络安全培训； |  |
| 10 | 档案整理 | 项目结束后对全部资料归档整理，并移交甲方。 |  |

**（二）服务要求**

1.协助建立演习组织指挥中心，负责演习的统一部署、组织协调和过程控制，确保演习工作安全推进，达到预期目标。

2.制定完善的对抗演习方案，成立演练工作组，明确人员分工及攻击方和防守方规则和要求。

3.演习前，对防守方进行安全检查加固指导，以便做好防守准备。对攻击方进行安全检查，确保攻击行为安全可控。演习时，中标方全程派人值守，确保出现问题第一时间解决，第一时间配合应急处置，做好现场秩序管理和服务支持。演习结束，攻方停止攻击，协助各参演企业进行系统功能测试，确保经过演习，各系统使用正常。检查攻击方数据、彻底清除演练数据回收相关资料，确保数据安全。

4.详细记录演习双方演练过程数据，向指挥人员、参观人员介绍对战过程，展示各项数据信息。对演练进行全面总结，公布问题、分析原因、提出整改建议。提交工作总结报告。

5.对演习过程中检测出的安全漏洞及隐患做好保密，仅提供甲方整改使用，确保攻击方不留存、不传播、不利用。

6.指导甲方系统恢复运行、漏洞修复及整改加固。

7.如有实际需求调整，经甲乙双方协商后开展。

六、比选原则及主要方法

**（一）比选采用综合评分法**

|  |  |  |
| --- | --- | --- |
| **评分项目** | **分值** | **评分标准** |
| 投标报价 | 10 | 投标人的价格分统一按下列公示计算：投标报价得分＝（评标基准价/投标报价）×10。评标基准价是指满足招标文件要求且投标价格最低的投标报价。除低于成本价的投标报价被拒绝外，最低报价得10分,得分结果由高分到低分依次排列为各自最终得分。 |
| 技术方案内容（50分） | 演习方案（30） | 攻防演练方案中包含：  （1）前期准备阶段，4分；  （2）组织策划阶段，5分；  （3）攻防实施阶段，6分；  （4）风险识别和应急处置，6分；  （5）演习总结阶段，6分；  （6）保密方案，3分。  1.方案内容全面且描述精确细致，具体落实体现，合理性强，能够满足要求得30分。  2.（1）-（6）每缺少一项或每有一项未按要求提供内容扣对应分值，扣完为止。  3.方案内容中每出现一处缺陷或不足的扣1分，扣完为止。 |
| 演练平台（20分） | 演练平台要求：  （1）组网准备。为保证攻防活动中攻防双方正常使用攻防平台系统、稳定进行网络访问，并根据坐落位置进行布设走线4分。  （2）基础资源准备。提供统一的演习通道（VPN或堡垒机等设备），为攻击方和防守方分配账号，4分。  （3）全程录屏录像监控。全程监控攻击终端所有运行的进程，演习场地录像，4分。  （4）全程审计。对攻击流量进行全流量监测和实时审计，发现异常攻击行为和风险时，及时预警并阻断，4分。  （5）演练平台提供实况展示，在演练期间通过大屏进行展示攻击和防守情况，4分。  1.演练平台所有功能能具体落实体现，能够满足要求得 20 分。  2.（1）-（5）每缺少一项或每有一项未按要求提供内容扣对应分值，扣完为止；  3.方案内容中每出现一处缺陷或不足的扣 1 分，扣完为止。 |
| 业绩 | 5 | 投标人自2019年1月1日（时间以合同签订时间为准）以来，承接过类似项目业绩，每提供一个得2.5分，满分5分，未提供或不符合不得分。  （以投标文件所附合同或证明材料的扫描件或复印件加盖公章为依据，未提供不得分） |
| 团队服务能力 | 10 | 投标人须配备的攻击队伍，配备5支及以上队伍有参加过网络安全赛事经验的，得5分；4支队伍参加过网络安全赛事经验的，得4分；3支队伍参加过网络安全赛事经验的，得 3分；其它不得分。  项目成员/团队/组织在相关网络安全赛事有获奖证明材料或表彰材料的，每有1 项得 1分，满分5分。  评审依据：以投标文件所附相关证明的扫描件或复印件加盖投标人电子公章，未提供或不符合不得分。 |
| 10 | 1、投入本项目的项目经理，具有PMP、注册信息安全工程师（CISP）、信息系统安全专业认证（CISSP）、系统集成项目管理工程师证书，每有一项得0.5分，满分2分。  2、项目团队成员中须具有系统架构设计师、注册信息安全工程师（CISP）、高级软件工程师、系统集成项目管理工程师证书，每有一项得2分，满分8分。  评审依据：提供相关人员证书扫描件并加盖投标人电子公章，未提供或提供无效不得分。  注：以上人员不可重复得分。提供上述人员对应评分项要求的证书复印件或扫描件，同时提供投标人为其缴纳的近半年内连续3个月社保证明材料作为佐证，未提供对应项分值不得分。 |
| 资信能力 | 15 | 1.投标人具有质量管理体系认证、环境管理体系认证、职业健康安全管理体系认证，每具有一项得1分，最高得3分。  2.投标人具有CMMI5级证书得3分，CMMI4级证书得2分，CMMI3级证书得1分，未提供不得分。  3.投标人具有中国网络安全审查技术与认证中心颁发的信息系统安全集成服务证书一级得3分，二级得2分，三级1分未提供不得分。  4.投标人具有中国网络安全审查技术与认证中心颁发的信息安全应急处理服务证书一级得3分，二级得2分，三级1分未提供不得分。  5.投标人具有中国网络安全审查技术与认证中心颁发的信息安全风险评估证书一级得3分，二级得2分，三级1分，未提供不得分。  评审依据：提供认证证书扫描件并加盖投标人电子公章。 |

**（二）中选人、中选价的确定**

1、按本办法比选，评标结果按评审后得分由高到低顺序排列。得分相同的，按修正和扣除后的投标报价由低到高顺序排列。得分与投标报价均相同的处理方式：并列。

2、比选人应确定排名第一的中选候选人为中选人，如中选人因不可抗力或无故提出不能履行合同，比选人可以确定排名第二的中选候选人为中选人，依此类推。

3、中选人确定后，中选价即中选人参选报价。经过监督单位确认的中选人由科技和信息化局进行公示，公示期为3日历天，公示期后直接签订委托合同。

联系人：张腾龙 0951-5918376

附件：1.确认函

2.法定代表人授权书

宁东基地管委会科技和信息化局

2023年5月15日

附件1

报价函格式

宁东基地管委会科技和信息化局：

一、我单位全面研究了你单位发布的比选文件，决定参加你单位组织的（项目名称）比选。我方授权（姓名、职务）代表我方（参选单位的名称）全权处理本项目比选的有关事宜。

二、一旦我方中选，我方将严格履行协议书、合同及比选文件规定的责任和义务。

三、一旦我方中选，将严格履行合同规定的责任和义务，保证于合同签字生效后按合同要求完成委托内容。

四、保证我方已提供和将要提供的文件资料是真实、准确、完整的。若比选过程中查有虚假，同意作废参选文件，若中选之后查有虚假，同意被废除中选资格。

本次我方参选报价为：

参选单位名称（盖章）：

参选单位授权代理人姓名或法定代表人（签字）：

联系电话：

附件2

法定代表人授权书

宁东基地管委会科技和信息化局：

本人系（参选人名称）的法定代表人，现委托我公司XX（其在本公司的职务是：XXX， 联系电话： XXXXXXXXXXX，手机：XXXXXXXXXXX，传真：/ ，身份证号： XXXXXXXXXXX）为我方代理人，代表我公司全权处理（项目名称）比选的一切事项，若中选则全权代表本公司签订合同，并负责处理合同履行等事宜。

本委托书有效期：自 XXXX年XX月XX日起至 XXXX年XX月XX日止。代理人无转委托权。

特此声明。

法定代表人签字盖章：

身份证号码：

代理人被授权人签字盖章：

身份证号码：

日期：