合同编号：

北京市数字农业农村促进中心

合同名称：信息系统运维类项目（网络安全保障服务项目）01包-安全保障服务采购项目

甲方：北京市数字农业农村促进中心

乙方：北京华胜天成科技股份有限公司

合同编号：

签约地点：北京

签约日期：2026年 6月 8日

1. 合同说明条款

1.1 甲方的“ 信息系统运维类项目（网络安全保障服务项目）01 包-安全保障服务采购项目 ”以公开招标（编号：BJJQ-2026-370/01）的方式采购，确定“北京华胜天成科技股份有限公司”为“信息系统运维类项目（网络安全保障服务项目）01 包-安全保障服务采购项目”服务方（即乙方）。依据《中华人民共和国民法典》，甲乙双方同意按照下面的条款和条件，签订本合同。

1.2 甲、乙双方之间任何与本合同有关的信函、电子邮件、电话，均应使用并且只能使用下列双方确认的地址、电话号码、传真号码、电子邮箱。前述地址同时为双方将来发生诉讼时法院送达司法文书的地址。任何一方变更通讯信息的，应在变更前 3 日内书面通知相对方，变更通讯信息一方未依约通知相对方的，相对方按照本合同所列通讯信息发出通知，无论变更一方是否收到，通知发出当日视为已送达，由此产生的一切责任由变更通讯方式一方承担。

	地址	电话	传真	电子邮箱
甲方	北京市通州区留庄路 5 号院 1 号楼	010-55525438	010-55525414	JinShy@nyncj.beijing.gov.cn
乙方	北京市海淀区西北旺东路 10 号院东区 23 号楼 5 层 501	18601366988	010-80986698	wangfang@teamsun.com.cn

1.3 甲、乙双方之间有关合同的财务往来及结算，应通过下列甲方与乙方共同确认的银行及账号进行。本合同存续期间，乙方若遇结算银行及账号变化，应提前 3 日书面告知甲方。若因乙方未及时提供变更后的银行账号导致甲方付款延迟的，甲方不承担任何违约责任。

甲方开票信息：

单位：	北京市数字农业农村促进中心
纳税人识别号：	12110000MB1J74594J
账号：	20000054675100070634689
开户行：	北京银行潞城支行

乙方银行账号信息：

单位：	北京华胜天成科技股份有限公司
账号：	610777555

开户行：	民生银行北京万柳支行

1.4 本合同的有效组成部分包括：本合同正文及附件、招标文件澄清及招标文件、投标文件澄清及投标文件等。如上述文件的内容产生冲突或矛盾，在不背离招标文件实质内容的前提下，将以本合同文档为准。

2. 合同技术内容

北京市农业农村局引入一系列信息安全服务工作，从管理、技术、运维、保障多个维度，借助专业的安全服务对网络、系统、设备、数据等多个层面加强信息系统的安全，保障安全稳定运行。

安全运维服务包括：物理资源运维服务、信息安全运维服务。（详见附件二）

物理资源服务是对已过保的防火墙、VPN 等安全设备提供续保服务，确保硬件平台持续稳定运行。

攻击面收缩包括公网 IP 暴露资产清查、外网开放端口筛查、高危服务暴露排查、无效域名解析清理等。

内部红蓝攻防演练防守包括攻击流量分析、威胁研判、溯源分析等工作。在演习结束后进行全面复盘总结，出具正式专项总结报告。

内容包括攻防数据统计、被攻击点位汇总、防守问题清单、现有安全体系缺陷、设备策略漏洞、风险隐患明细。针对所有问题逐条制定可落地的整改方案、加固措施、优化计划完成逐项整改和闭环销号。

技术检测包括按照网络安全、数据安全检查单位检查要求，开展委局业务系统的安全技术自查，做好技术支持，将检查中出现的问题进行整改，提供工作建议。

漏洞专项治理包括定期对委局各系统和各终端安全漏洞进行发现、评估工作，评估各系统漏洞治理成效。通过主动排查隐患、动态跟踪漏洞态势等手段，及时发现安全隐患，并提出整改意见和建议，督促整改。

渗透测试主要是对委局所有系统采用可控、非破坏性的测试方法对网络、主机、服务器以及数据库应用等测试目标进行检测。

网络安全和数据安全评估从网络架构安全、主机安全、应用安全、数据安全、人员安全意识、制度体系建设等维度开展全面评估。重点核查安全策略规范性、

资产防护全覆盖性、风险管控闭环性、合规资料完整性，排查架构性短板、体系性漏洞、管理类隐患、流程性缺陷。评估完成后输出正式《网络安全风险评估报告》《数据安全风险评估报告》，梳理整体安全现状、现存风险清单、合规偏差项、体系薄弱点，出具中长期安全优化整改建议、架构优化方案、制度完善计划，提供权威技术依据。

3. 合同技术要求

乙方按照本合同提供服务期间，通过常态化安全服务保障信息系统持续稳定、可靠运行。通过应急保障相关服务确保一旦发生安全事件，及时处置，降低事件造成的危害。通过数据安全服务保障数据资产安全，以满足“事前可预防、事中可控制、事后可恢复”的信息安全保障需求，打造一个可信、可管、可控、可视的环境，保障北京市农业农村局重要信息系统、网络及终端设备持续安全稳定运行。

物理资源服务技术要求:

设备硬件、软件故障处置闭环率 100%, 定期完成设备状态巡检、隐患排查、加固优化，无因维保缺失导致的设备失效、安全事故。

驻场运维技术要求：

（1）**常态化巡检：**

落实月、季、年全维度巡检机制，每月梳理账号权限、安全策略、端口映射；每季度开展漏洞扫描、基线核查；每年完成合规自查与整体安全复盘，所有巡检问题当日处置、按期闭环。

攻击面收缩服务：

全面清查公网暴露资产、开放端口、外网映射、无效域名服务，批量关停非必要暴露资产与高危服务，收敛内网高危端口与匿名访问权限，实现外网最小暴露、内网最小权限，从源头降低入侵风险，形成清查、整改、复测、台账闭环管理。

内部红蓝对抗保障：

模拟外网渗透、内网横向攻击、权限提升、数据窃取等真实场景，检验防护体系与人员防守能力，赛后梳理防守短板、策略缺陷，落地优化加固措施。

漏洞专项治理服务：

针对高危、重复、顽固合规漏洞开展专项攻坚治理，覆盖全品类信息化资产，通过工具扫描+人工复核方式精准定位隐患，落实分级整改机制，高危漏洞即时清零、中低危漏洞限期闭环。

渗透测试服务：

定期开展合规授权渗透测试，模拟真实黑客攻击场景，挖掘常规巡检无法发现的隐性漏洞、业务逻辑缺陷、深层权限漏洞，全程不影响业务运行、不破坏数据，测试后提供详细漏洞报告、复现步骤、加固方案，并协助完成全量整改复测闭环，高危漏洞、重大安全隐患整改闭环率 100%。

安全评估服务：

参照等保 2.0 及行业标准，从网络架构、设备配置、边界防护、主机应用、数据安全、运维管理、应急能力等多维度开展整体安全评估，排查架构性、体系性、管理性风险，输出风险评估报告与中长期安全优化整改方案。

4. 服务期限及履行地点

服务期限： 自合同生效之日起 12 个月。

履行地点：甲方指定地点。

5. 费用支付或结算方式

5.1 费用合计

本合同的费用合计为人民币（大写）：贰佰肆拾玖万伍仟元整（¥：2495000.00 元）。

详细分项报价见附件一：分项报价表

5.2 支付方式

5.2.1 首付款：本合同签署后，财政拨款到账后，甲方向乙方支付合同款总额的 50 %，人民币大写：壹佰贰拾肆万柒仟伍佰元整；小写：¥ 1247500.00 元。

第二次付款：甲方于 2026 年 9 月 30 日前，对乙方初步考核合格后，向乙方支付合同款总额的 40 %，人民币大写： 玖拾玖万捌仟元整 ；小写：¥ 998000.00 元。

第三次付款：甲方于 2027 年 6 月 30 日前，在乙方提供的服务验收合格的情况下，向乙方支付合同款总额的 10 %，人民币大写： 贰拾肆万玖仟伍佰元

整；小写：￥ 249500.00 元。

5.2.2 乙方应在甲方支付每期价款之前提供等额正式发票。若乙方怠于提供发票或提供的发票不符合甲方的要求，甲方有权迟延付款且不承担违约责任。

5.2.3 因财政国库的原因导致甲方不能按时付款的，甲方有权顺延付款，且不承担违约责任。

6 验收标准和方式

6.1 验收时间：服务期限届满之日起 10 个工作日内，乙方提供的服务最迟应通过验收的时间： 2027 年 6 月 30 日前。

6.2 验收标准：

此处要明确验收标准，如国标、行标或技术标准、服务标准或达到的技术要求。

6.3 乙方完成安全服务后应及时通知甲方（以书面形式发送验收申请至甲方）进行验收，并提供相关验收材料。验收合格的，甲方联系人在验收合格单上签字。验收不合格的，乙方须对甲方在验收过程中指出的问题进行整改，并于 3 个工作日后重新申请验收，直至验收通过。

6.4 验收材料清单如下：

序号	项目验收材料	数量	材料形式	提交时间
1	《故障处理报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
2	《技术支持报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
3	《安全监测报告》	52 份	纸质版/电子版	2027 年 6 月 20 日
4	《安全事件应急处置报告》	按需	纸质版/电子版	2027 年 6 月 20 日
5	《资产风险分析报告》	2 份	纸质版/电子版	2027 年 6 月 20 日
6	《红蓝对抗演练实施方案》	1 份	纸质版/电子版	2027 年 6 月 20 日
7	《红蓝对抗演练总结报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
8	《安全应急演练方案》	2 份	纸质版/电子版	2027 年 6 月 20 日
9	《安全应急演练总结	2 份	纸质版/电子版	2027 年 6 月 20 日

	报告》			
10	《演习期间网络安全监测报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
11	《安全应急处置报告》	按需	纸质版/电子版	2027 年 6 月 20 日
12	《网络安全演习总结报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
13	《委局业务系统安全技术检查报告》	4 份	纸质版/电子版	2027 年 6 月 20 日
14	《委局业务系统技术检查年度报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
15	《漏洞扫描报告》	4 份	纸质版/电子版	2027 年 6 月 20 日
16	《漏洞治理年度报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
17	《渗透测试技术方案》	2 套	纸质版/电子版	2027 年 6 月 20 日
18	《渗透测试实施方案》	2 套	纸质版/电子版	2027 年 6 月 20 日
19	《渗透测试报告》	2 套	纸质版/电子版	2027 年 6 月 20 日
20	《网络安全风险评估技术方案》	1 份	纸质版/电子版	2027 年 6 月 20 日
21	《数据安全风险评估方案》	1 份	纸质版/电子版	2027 年 6 月 20 日
22	《网络安全风险评估实施方案》	1 份	纸质版/电子版	2027 年 6 月 20 日
23	《数据安全风险评估实施方案》	1 份	纸质版/电子版	2027 年 6 月 20 日
24	《网络安全风险评估报告》	1 份	纸质版/电子版	2027 年 6 月 20 日
25	《数据安全风险评估报告》	1 份	纸质版/电子版	2027 年 6 月 20 日

7. 服务响应

为了更好地为甲方提供服务，乙方应：

7.1 要求乙方提供 7 天*24 小时在线服务。乙方在接到甲方通过电话、信函、传真、电子邮件、网上提交等方式提出的服务请求后，应在 4 个小时之内给予响应并提供服务。

7.2 乙方技术人员到达服务现场后，应在 4 小时内解决甲方问题，确保甲方业务能够正常开展。

8 保密条款

禁止乙方泄露本合同所涉及的甲方相关商业和技术秘密。保密条款之时效将不受本合同有效期的影响，本合同服务期满后 10 年内该保密条款仍将有效。

9 甲方的权利义务

9.1 甲方有权对乙方提供的与本合同相关的服务情况进行监督和检查。

9.2 甲方应有权对乙方服务人员的工作态度、工作完成情况及工作方案提出改进建议。

9.3 甲方应按照本合同议定的条款向乙方支付合同款。

9.4 甲方有权了解乙方向甲方提供的服务技术细节。

9.5 甲方有权了解乙方关于服务的管理制度。

9.6 甲方有权向乙方提出更换服务人员的要求。

10 乙方的权利义务

10.1 乙方应按照本合同约定向甲方提供服务，并遵守国家法律法规及甲方的各项工作制度和相关要求。乙方应具有提供本合同约定的服务的资质和能力，并向甲方提供加盖乙方公章的资质证明文件的复印件作为本合同附件。

10.2 乙方在项目实施前，应于 2026 年 6 月 10 日前制定详细的服务方案或实施计划，并经甲方确认后方可实施。

10.3 乙方保证其向甲方提供的合同不存在任何侵犯第三方著作权、商标权、专利权等知识产权的情形，否则乙方应赔偿因此给甲方造成的全部损失。

10.4 乙方应保证为甲方提供服务的人员具备提供本合同要求所需的相应资质和许可，并保证乙方人员在为甲方提供合同要求的过程中，严格遵守甲方的各项规定。

10.5 如因乙方人员原因，给甲方或第三方造成人员人身伤害或财产损失的，乙方应自行承担赔偿责任。

10.6 未经甲方的书面许可，乙方不得以任何形式将其在本合同项下的权利义

务转让给任何第三方。

10.7 乙方负责对甲方所需的基本知识提供相关的培训，以便可以更好地为甲方服务。

11 违约责任

11.1 甲乙双方均应全面履行本合同，任何一方不履行或不按约定履行均构成违约，违约方应赔偿因此给对方造成的全部损失，包括但不限于另一方的直接损失、可得利益损失以及另一方为维护自身合法权益而支付的诉讼费、律师费、公证费、公告费、保全费、财产保全责任保险费、鉴定费等合理费用。

11.2 乙方逾期向甲方提供服务，或逾期响应甲方的服务要求，或逾期交付材料，或逾期通过验收的，每迟延一日，乙方应向甲方支付本合同项下合同款总额千分之二的违约金；迟延 15 日的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付合同款总额 10 %的违约金，前述违约金不足以弥补甲方损失的，甲方有权向乙方继续追偿。

11.3 乙方提供的服务不符合本合同约定标准的，乙方应当在甲方规定的期限内进行返工或采取补救措施，并重新提交甲方验收；如乙方提供的服务经二次验收仍验收不合格，或乙方拒绝按照甲方要求进行返工或采取补救措施的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付合同款总额 10%的违约金，前述违约金不足以弥补甲方损失的，甲方有权向乙方继续追偿。

11.4 除上述违约情形外，如乙方违反本合同约定的任何义务，甲方有权向乙方发送通知要求乙方按本合同约定履行义务。如乙方在甲方通知指定期限内未按本合同约定履行义务的，甲方有权解除本合同，要求乙方退还甲方已支付的全部款项，乙方还应按照本合同总价款的 10%向甲方支付违约金，前述违约金不足以弥补甲方损失的，甲方有权向乙方继续追偿。

12 不可抗力

12.1 双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

12.2 受不可抗力影响的一方应在不可抗力的事件发生后 10 天内以书面形式通知另一方。

12.3 因不可抗力致使本合同不能履行的，经双方协商一致，本合同终止。

13 解决合同纠纷的方式

甲乙双方应通过友好协商，解决在履行本合同中所发生的或与本合同有关的一切争端，如果协商仍得不到解决，双方中任何一方均可向甲方所在地有管辖权的人民法院起诉。

14 廉政承诺

合同双方承诺共同加强廉洁自律、反对商业贿赂。

15 其他

15.1 本合同正本一式 7 份，以中文书写，经双方盖章、签字后即生效，甲方 4 份,乙方 3 份，具有同等法律效力。

15.2 合同履行过程中，如需修改或补充合同内容，经协商一致，双方应签署补充协议，该协议将作为本合同不可分割的一部分，并具有同等法律效力。

15.3 本合同签订及履行适用中华人民共和国相关法律法规等有关规定。

甲方：北京市数字农业农村促进中心(盖章)

法定代表人或授权代表：

（签字）

联系人：

2026年 6月 8日

乙方：北京华胜天成科技股份有限公司(盖章)

法定代表人或授权代表：

（签字）

联系人：

2026年 6月 8日

附件一：分项报价表

投标分项报价表

项目编号/包号：BJJQ-2026-370/01 项目名称：信息系统运维类项目（网络安全保障服务项目）报价单位：人民币元

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	设备维护（设备续保服务）	30000.00	1	30000.00	无
2	驻场服务	350000.00	1	350000.00	无
3	攻击面收缩服务	330000.00	1	330000.00	无
4	内部红蓝对抗蓝队防守工作	250000.00	1	250000.00	无
5	安全应急演练	70000.00	1	70000.00	无
6	演习期间分析研判	55000.00	1	55000.00	无
7	演习期间应急处置	45000.00	1	45000.00	无
8	演习总结与整改	10000.00	1	10000.00	无
9	安全技术检查	70000.00	1	70000.00	无
10	安全漏洞治理	270000.00	1	270000.00	无
11	制定渗透测试方案	60000.00	1	60000.00	无
12	渗透测试实施	500000.00	1	500000.00	无
13	渗透测试整改结果检查	85000.00	1	85000.00	无
14	制定安全评估方案	90000.00	1	90000.00	无
15	现场安全评估实施	220000.00	1	220000.00	无
16	安全评估总结和整改	60000.00	1	60000.00	无
总价（元）				2495000.00	无

附件二： 服务内容与标准

一、概述

为全面落实《中华人民共和国网络安全法》《党委（党组）网络安全工作责任制实施办法》等有关法律规定，保障中共北京市委农村工作委员会、北京市农业农村局（以下简称“委局”）网络、重要信息系统和业务数据安全防护水平，确保委局各项业务的正常开展，由专业安全运维团队构建多层次、多纵深防护体系，对发现的薄弱环节进行整改加固，重点提升委局的安全隐患识别、预警和治理能力，攻击检测响应、实战攻防保障能力，全力保障委局网络和系统安全。

二、项目目标

依托安全服务机构所提供的专业化信息安全服务，构建安全保障体系，不断增强安全防护能力、隐患检测能力和恢复能力，并确保符合国家及北京市网络安全工作相关要求，满足“事前可预防、事中可控制、事后可恢复”的信息安全保障需求，打造一个可信、可管、可控、可视的环境，保障北京市农业农村局重要信息系统、网络及终端设备持续安全稳定运行，为委局业务的高效、顺利开展提供有力支撑。

三、项目原则

为实现信息系统运维类项目（网络安全保障服务项目）的总体目标，结合委局实际情况和未来发展需求，在开展本项目运维工作的时候，将贯彻以下服务原则。

3.1 合法合规需求。项目实施需遵守以下法律和制度：

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）相关要求；

《中华人民共和国网络安全法》相关要求；

《中华人民共和国数据安全法》相关要求：

《中华人民共和国个人信息保护法》相关要求；

《关键信息基础设施安全保护条例》相关要求；

《网络数据安全管理条例》相关要求；

《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》相关要求；

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）相关要求；

《公共互联网网络安全威胁监测与处置办法》相关要求；

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）相关要求；

《信息安全技术 代码安全审计规范》（GB/T 39412-2020）相关要求；

《信息安全技术 网络脆弱性扫描产品安全技术要求》（GB/T 20278-2022）相关要求；

《信息安全技术 终端计算机通用安全技术要求和测试评价方法》（GB/T 29240-2024）相关要求；

《信息安全技术 网络安全服务能力要求》（GB/T 32914-2023）相关要求。

3.2.先进性与实用性原则

在充分利用已有设备、保护先期投资的基础上，采用先进、成熟、实用的技术和设备，维护和运行监管委局信息系统。

3.3.标准化与规范化原则。项目实施须由专业安全服务人员依照规范的操作流程进行。

3.4.最小影响原则。安全运维服务工作尽可能小的影响系统和网络的正常运行。

3.5.技术与管理相结合原则。安全运维须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

3.6.可控性原则。安全服务的工具、方法和过程要在双方认可的范围之内，保证北京市农业农村局对于服务过程的可控性。

四、主要工作内容

北京市农业农村局引入一系列信息安全服务工作，从管理、技术、运维、保障多个维度，借助专业的安全服务对网络、系统、设备、数据等多个层面加强信息系统的安全，保障安全稳定运行。

安全运维服务包括：物理资源运维服务、信息安全运维服务。

物理资源服务是对已过保的防火墙、VPN 等安全设备提供续保服务，确保硬件平台持续稳定运行。

信息安全运维服务中，驻场服务服务保障了信息系统持续稳定、可靠运行，

并确保一旦发生安全事件，及时处置，降低事件造成的危害；在网络安全演习保障服务部分，通过攻击面收缩服务、内部红蓝对抗、安全应急演练、演习期间分析研判、演习期间应急处置、演习总结与整改等多个阶段，有效提升客户网络安全实战能力。在漏洞专项治理、渗透测试、网络安全评估服务部分，包含了三项内容，分别为安全漏洞专项治理，渗透测试，委局网络安全和数据安全评估。通过第三方专业的咨询团队提供技术支撑，提高委局的网络安全水平，降低安全风险，保障业务连续性和合规性。

五、详细服务内容及要求

服务内容包含北京市农业农村局相关信息系统及网站、云主机及终端设备，具体数量如下：

市级政务云已经完成部署的信息系统，所有设备近 200 台云主机、14 个在链系统及网站、副中心办公区 600 余台终端设备。

乙方需至少提供 2 名驻场人员，现场提供 5×8 小时安全咨询支撑及安全运维服务。服务内容项见表 1。

表 1-----服务内容项

<table>
<tr><th>序号</th><th>服务名称</th><th>技术指标要求</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">设备维护（设备续保服务）</td><td>针对过保设备提供设备续保服务。</td></tr>
<tr><td>服务范围：北京市农业农村局的相关安全设备。
安全设备汇总表如下：
<table>
<tr><th>序号</th><th>名称</th><th>数量</th></tr>
<tr><td>1</td><td>防火墙 NGFW4000-UF（TG-5330）-防火墙</td><td>2</td></tr>
<tr><td>2</td><td>TOP VPN6000 (TV-6514-VONE)</td><td>1</td></tr>
</table>
服务响应：每周 7×24 小时。2 小时内抵达现场；
服务内容：硬件保修、故障处理、软件升级。
服务频率：开展 1 年安全设备续保和带宽管理服务。
服务成果：提交（包括但不限于）如下文档，《故障处理报告》《技术支持报告》。</td></tr>
<tr><td>2</td><td>驻场服务</td><td>开展委局系统安全监测、提供委局系统安全 7*24 应急响应，5*8 小时驻场服务，服务团队包含 1 名组长、1 名组员。组长负责</td></tr>
</table>

		统筹监测分析工作，规划好监测范围和重点，协调各方监测。对安全事件进行深层技术分析，评估影响，制定应急策略，总结经验改进。组员负责负责日常监测，及时上报异常。安全事件发生时进行应急响应，配合组长调查。密切关注网络流量、网络日志、网络运行状态、防范网页篡改、勒索攻击、域名劫持等重大威胁。
		服务范围：委局业务系统。 服务频率：服务期限内持续性开展。 服务成果：每周提交《安全监测报告》，安全事件处置完成后提供《安全事件应急处置报告》。
3	攻击面收缩服务	进行全面的资产清查，与各系统业务方充分沟通，梳理所有可能的攻击面，明确潜在风险区域。 技术检测阶段，专业人员仔细检测和识别委局暴露在互联网上的资产数据、端口信息、敏感信息，编制详尽的攻击暴露面报告，并与业务方交流确认，确保报告准确反映实际情况。 风险分析时，深入研讨暴露在互联网中的风险，结合业务需求与各系统业务方共同制定应对策略。 在攻击面收缩环节，技术支持队伍全力提供技术支撑，确保修复工作高效进行。同时，持续监控风险状况，与业务方紧密合作，不断调整防护措施，切实降低攻击面，提升系统安全性。具体要求如下： （1）对委局互联网资产进行全面清查，与各系统业务方充分沟通，梳理所有可能的攻击面，明确潜在风险区域。资产暴露面数据内容包括但不限于：WHOIS 数据、域名数据、ICP 备案数据、DNS 服务器、APP 移动应用、公众号/小程序、公共代码仓库 GIT/GITLAB、微博/微信等社交媒体公开信息、开发者社区信息、电子邮件地址等。 （2）对委局政务外网资产进行全面清查，梳理所有可能的攻击面，明确潜在风险区域。资产暴露面数据内容包括但不限于：资产开放的端口信息、协议信息、敏感数据、资产漏洞等。

		（3）暴露面工作梳理完成后，对采集的数据进行风险分析，深入研讨资产暴露在互联网中的风险，结合业务需求与各系统业务方共同制定应对策略。 （4）提供资产暴露面检测工具，工具的部署不能对现有网络系统造成影响。 （5）结合委局工作安排，每年开展 2 次攻击面收缩服务，形成相应的报告。
		服务范围：委局互联网对外业务系统。 服务频率：服务期限内开展 2 次。 服务成果：提交《资产风险分析报告》2 份。
4	内部红蓝对抗蓝队防守工作	分析并梳理委局业务系统安全和数据安全现状，如漏洞情况、防护措施等，统筹编制红蓝对抗计划与方案，组建防守队、组建红蓝对抗期间现场支持队伍，开展红蓝对抗攻防演练，对委局整体安全防御情况进行模拟防守。通过蓝队防守，深入评估和发现委局的安全防护短板。此外，结合当前网络安全体系，提出改进建议。对演练结果形成问题清单反馈并总结。
		服务范围：委局业务系统 服务频率：服务期限内开展不少于 1 次，为期 5 天。 服务成果：提交《红蓝对抗演练实施方案》1 份、《红蓝对抗演练总结报告》1 份。
5	安全应急演练	积极与各系统业务方进行沟通，充分了解业务需求和安全关注点，以便更好地制定针对性的演练方案。 编制应急演练计划与流程，同时组建现场技术支持队伍，为演练提供技术层面的支持与协助。 通过实战或者模拟各种网络安全事件，检验系统应急响应能力。在演练过程中，及时与各系统业务方交流反馈情况，共同探讨应对策略。对演练结果总结反馈，形成问题清单，并与各系统业务方共同商议改进措施，提升系统安全性。具体要求如下所述： 在服务期内每年开展网络安全应急演练，网络安全事件场景包

		括但不限于网页被篡改、系统中病毒、数据库误操作、数据泄漏等。通过开展应急演练，检验评估委局当前网络安全事件应急预案流程、机制的可操作性、实用性。网络安全应急演练开展内容包括演练前期准备、实施、总结各阶段相关工作。 • 演练前期准备：结合委局需求，梳理常见网络安全突发事件场景并设计编制相应场景的演练方案、脚本，明确演练目标、范围、计划以及人员安排。组织委局相关部门人员进行演练前的动员及培训，确保参演人员掌握演练规则、应急流程以及应急知识。同时，准备好演练所需硬件设备、软件工具、模拟数据等资源，搭建演练环境，每次演练支撑人员不少于 3 人，保障演练的顺利开展。 • 应急演练实施：基于预设的网络安全事件场景演练方案和脚本，在安全可控的条件下模拟事件发生、进行演练解说。委局相关部门人员按照应急流程进行快速响应处置。 • 应急演练总结：演练结束后根据演练实施情况编制演练总结报告，评估本次演练组织实施的效果情况，包括响应速度、处置能力、问题及不足之处等。针对相关问题，提出合理、有效的改进提升建议，协助完善优化现有应急预案。 服务期内开展应急演练不少于 2 次，服务期内覆盖委局所有系统。
		服务范围：委局业务系统 服务频率：服务期内开展 2 次。 服务成果：提交《安全应急演练方案》2 份，《安全应急演练总结报告》2 份。
6	演习期间分析研判	在演习期间对委局业务系统安全告警信息进行分析和挖掘，对各类告警数据进行深层次分析，挖掘隐患、判断隐患威胁的严重程度，并对分析结果归类整理。具体要求如下所述： （1）在演习期间进行每日值守，对委局业务系统安全告警信息进行分析和挖掘，对各类告警数据进行深层次分析，挖掘隐患、判断隐患威胁的严重程度，并对分析结果归类整理。具体的值守时

		间参考国家攻防演练时间要求。 （2）在演练前对现有安全防护措施进行调研，针对不足的防护措施在演习期间提供对应的设备或平台，补齐防护的不足。 （3）多维度的信息和多源数据进行整合、关联、智能分析和预测，基于攻击意图、攻击策略、攻击方法、攻击次数、攻击时间、处置状态等影响因子构建资产评级模型，在大量资产中识别失陷资产；通过对网络数据包、文件元数据、终端日志、威胁情报、漏洞知识库等进行智能分析，洞悉攻击的人员、目标、时间、地点和手段，发现高级潜伏威胁。 （4）有效发现暴力破解攻击、拒绝服务攻击、扫描行为攻击等异常流量的检测；能够对 web 攻击、文件攻击、邮件威胁等进行实时的攻击预警；可与防火墙、EDR、WAF 等防护产品进行联动，实现各种控制行为的阻断防护。
		服务范围：委局业务系统 服务频率：服务期内开展不少于 1 次 服务成果：提交《演习期间网络安全监测报告》。
7	演习期间应急处置	在演习期间按照监测分析、事件研判、应急处置、联络协调进行分工分组，对异常事件处置，协助完成异常事件通报、研判、处置和事后分析等工作。
		服务范围：委局业务系统 服务频率：服务期内按需开展 服务成果：按需提供《安全应急处置报告》
8	演习总结与整改	演习完成后开展全面复盘总结，针对暴露出的漏洞、脆弱性等问题开展监督整改。具体要求如下所述： （1）演习期间完成每日防守工作总结，分析发现的安全问题、处置方案、下发的策略，提出改进建议，每日汇报工作。 （2）演习完成后应对整体的演习保障工作进行总结复盘，分析演习保障中存在的问题、不足，提供安全防护增强建议。
		服务范围：委局业务系统

		服务频率：服务期内开展不少于 1 次 服务成果：按需提供《网络安全演习总结报告》
9	安全技术检查	按照网络安全、数据安全检查单位检查要求，开展委局业务系统的安全技术自查，做好技术支持，将检查中出现的问题进行整改，提供工作建议。具体要求如下： （1）按照上级检查要求，开展委局范围内的系统和数据的安全技术自查。 （2）配合上级主管部门开展安全检查，做好技术支撑。 （3）重大活动和节假日等重点时期前，开展安全隐患排查。 （4）对自查和检查中发现的问题，给出整改建议，配合完成整改。 （5）对服务期内检查工作进行分析，并提出工作建议。 （6）支撑安全自查及配合迎检工作，确保业务系统满足上级监管单位要求的同时满足网络安全工作考核要求。
		服务范围：委局业务系统 服务频率：服务期内开展 4 次 服务成果：提供《委局业务系统安全技术检查报告》4 份、《委局业务系统技术检查年度报告》1 份
10	安全漏洞治理	通过自动化漏洞扫描工具和平台，结合委局工作安排，定期对委局各系统和各终端安全漏洞进行发现、评估工作，评估各系统漏洞治理成效。通过主动排查隐患、动态跟踪漏洞态势等手段，及时发现安全隐患，并提出整改意见和建议，督促整改。具体要求如下： 对指定的信息系统进行全面扫描与分析，检测工具的检测规则库及知识库应涵盖 CVE、CNCVE、CNVD、CNNVD 等标准。通过工具扫描发现信息系统安全隐患、数据库、中间件等存在的漏洞，分析漏洞和配置缺失等。 工具自动化扫描完成后，人工验证所发现的系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题，并评估漏洞风险程度。此外，针对漏洞扫描中出现的问题，提供针对性的安全修

		复建议，协助进行解决，并进行修复后再次复测工作。 服务期内开展漏洞扫描不少于 4 次，每次覆盖所有指定系统和终端。
		服务范围：委局业务系统 服务频率：服务期内开展不少于 4 次 服务成果：提供《漏洞扫描报告》4 份、《漏洞治理年度报告》1 份。
11	制定渗透测试方案	统筹考虑我市重大活动安全保障要求和委局工作安排，服务期内开展至少 2 次委局范围内全量系统的渗透测试，服务期内覆盖委局所有系统。 与各系统业务方沟通收集系统软件架构、开发语言、可用性要求、相关服务器、网络拓扑、设备部署情况等基本资料，确定目标与范围。确定关键漏洞与高风险区域。基于此制定渗透策略，考虑多种渗透路径与场景。最后对方案进行审核与完善，确保方案具有可行性与有效性，为后续渗透测试提供准确指导。
		服务范围：委局业务系统 服务频率：服务期内开展 2 次 服务成果：提供《渗透测试技术方案》2 套
12	渗透测试实施	服务期内需覆盖委局所有系统。与系统负责部门和相关责任人充分沟通确认，明确渗透测试的实施人员、时间、测试内容和配合事项等，专业技术人员采用可控、非破坏性的测试方法对网络、主机、服务器以及数据库应用等测试目标进行检测。
		服务范围：委局业务系统 服务频率：服务期内开展 2 次 服务成果：提供《渗透测试实施方案》2 套
13	渗透测试整改结果检查	针对所发现的问题提出相应的安全改进建议，以指导、监督应用系统开发商、运维服务商进行整改并及时复测。根据渗透测试所发现的安全漏洞编写检测报告。
		服务范围：委局业务系统

		服务频率：服务期内开展 2 次 服务成果：提供《渗透测试报告》2 套
14	制定安全评估方案	对委局所有平台和系统及其相关数据、人员、制度等，开展资产识别、威胁识别、安全措施识别、脆弱性识别，收集并整理相关文档，为评估提供基础资料。选择适合的评估方法，制定评估方案。
		服务范围：委局业务系统和数据 服务频率：服务期内开展 1 次 服务成果：提供《网络安全风险评估技术方案》1 份、《数据安全风险评估方案》1 份
15	现场安全评估实施	在现场安全评估实施中，深入分析收集的资料确定评估重点，实地查看物理安全措施、网络架构等，严格审查安全策略文件及执行情况，结合多方面结果评估风险。收集资料、整理信息。评估内容包括但不限于委局安全管理制度落实情况、网络安全状况、数据安全防护情况、敏感资产保护情况、人员安全管理情况、服务外包安全情况、应急保障情况等，并梳理和维护委局系统和数据资产清单、制度清单、风险清单和改进措施清单等。
		服务范围：委局业务系统和数据 服务频率：服务期内开展 1 次 服务成果：提供《网络安全风险评估实施方案》1 份、《数据安全风险评估实施方案》1 份
16	安全评估总结和整改	在现场安全评估后，全面总结与整改。对评估过程及结果进行深入整合，明确安全隐患与风险点，分析潜在影响并分类梳理。结合现场勘查、技术检测和安全策略审查等多方面信息，为整改提供准确依据。 在整改阶段，制定详细整改建议，指导整改过程，确保各项措施有效落实。
		服务范围：委局业务系统和数据 服务频率：服务期内开展 1 次 服务成果：提供《网络安全风险评估报告》1 份、《数据安全

		风险评估报告》1 份

六、项目实施与组织管理

6.1 人员要求

1) 项目管理人员能力要求

项目经理具有五年以上安全运维项目管理工作经验。具备范围管理、时间管理、质量管理、沟通管理等基本项目管理技能。具备领导团队经验，善于沟通、善于处理团队成员之间的关系。具有在其它政府部门或相关领域项目管理经验。思维清晰、敏捷，具有较强逻辑分析能力。

2) 驻场人员要求

除项目经理和技术负责人以外，不少于 1 人的全职支撑工作的驻场人员，能够服从采购人的工作安排，具备较强的专业素质，有优秀的书面表达能力、组织能力和沟通能力，具有与本项目类似网络安全保障项目经验。

3) 项目实施人员要求

服务单位必须向采购人提供拟派参加本项目的主要人员名单以及各自职责的划分。乙方必须向采购人保证中标后服务人员的稳定性，在本项目服务结束前，参加本项目的人员变动必须取得招标人同意。如因服务单位安排的项目组成员无法胜任相关工作，用户单位有权要求乙方无条件进行更换，直至能够胜任相关工作。

服务单位需为项目配备专属服务团队，同时拥有充足的安全专家资源、应用渗透专家及专业技术实施力量，可在项目关键阶段提供专业技术团队现场指导服务，必要时可邀请行业权威安全专家参与项目相关工作。乙方需明确项目核心人员配置与职责划分，保障项目团队严格依照实施方案开展工作。

乙方需为本项目配备项目经理和项目成员等角色：

1.项目经理需具备 5 年（含）以上工作经验。需具有良好的专业素质，具有丰富的项目全局把控和资源管理经验，负责总体设计、组织管理和协调，并作为本项目的实际主持者担负实质性工作；对政务部门信息化建设有充分了解，具有与本项目类似网络安全保障项目经验。

2.除项目经理外，需配备稳定的项目成员，并具有注册信息安全工程师 CISP 人员证书。专业结构及分组合理，覆盖项目所涵盖的业务领域，具备较强的调查

研究能力和组织实施能力，具有网络安全项目经验。

3 实施支撑人员

服务商需为项目提供强有力的后台技术支撑，可根据项目进展灵活调配人员力量，保障突发任务与关键节点工作的顺利推进。除项目核心管理、技术及驻场团队外，需配备充足的专业支撑人员，支撑团队全面覆盖项目全流程工作，分组设置科学合理，各组负责人专职专责，人员专业能力与岗位要求高度契合。

6.2 质量保障要求

应建立严格的质量保证体系，制定项目建设的质量控制方案和实施措施，并督促落实各环节质量控制内容和目标；保证项目各个阶段工作满足采购人对质量的要求。

6.3.安全保密要求

乙方应严格遵守合同规定，执行有关保密的法律法规，选派具有良好职业道德的人员参与和从事本项目工作，教育相关人员恪守职业道德，服从用户方的管理，严格遵守用户方的保密规定和工作制度，并承担相应的保密责任。乙方所有参与本项目的技术人员，对本项目涉及的所有系统数据（纸质文档、电子文档、光盘等）进行严格保密，都必须与用户方签订《保密承诺书》。乙方负责对《保密承诺书》归档保管，并接受用户方检查，乙方对承诺履行情况负有监督责任，一旦发现违反承诺情况，要及时向用户方报告。

6.4.项目时间要求

项目的运维期为：合同签订之日起 12 个月。

乙方须在合同签订之日起 12 个月期间完成本项目所有服务内容，乙方要按照服务内容的要求，制定具体的实施方案，做好进度和任务安排。做好与招标方前期工作的衔接，确保工作的平稳过渡，涉及费用及知识产权的按公平公正原则，由中标商自行协商解决，费用包含在投标报价中。

6.5 培训要求

本项目中开展安全培训工作，应对相关人员开展必要的安全培训，相关要求如下：

1.培训范围：中心指定人员。

2.培训目的：提升中心相关技术人员网络安全技术能力。

3.培训内容：

(1)提供 1 个 CISP 的培训认证。

(2)不少于 1 次的安全技术培训，如安全测试、攻防技术等内容，具体内容根据中心需求制定。

4.培训资料及语言

(1)培训资料：培训的全部内容都应提供详细的技术资料。

(2)培训语言：培训资料使用的文字为中文。

5.培训开展的方法

乙方应根据采购人的上述要求及乙方认为应予补充的内容制订一个详细的培训计划，并于培训开始前交给采购人，征求意见，以确保培训工作的顺利进行，达到预期的目的。

6.5.服务保障要求

要求乙方拥有一只稳定的服务保障队伍，并具有较强的技术保障实力，遇到突发情况时能够及时解决问题；服务团队有明确分工和侧重点，基本人员均掌握一般的安全服务方法并能解决常见设备的故障问题；具备提供每周 7×24 小时应急响应服务能力，针对设备出现的突发故障或问题，在 15 分钟内给予响应，2 小时内到现场，4 小时内予以解决。

6.6 项目验收及标准

本项目在服务完毕之日起 10 个工作日内，乙方要提供所有服务期内产生的纸质文档和电子文档,并向采购人提出最终验收申请，采购人组织项目验收工作。

验收的主要标准为:

1.满足采购服务要求的各项指标；

2.项目各项工作应交付的报告、服务、知识产权或成果符合项目预期；

3.项目文档齐全，项目管理过程合规，项目人员管理到位；

4.在规定时间内顺利通过专家验收评审。

验收流程:

1.采购人成立验收小组，根据合同条款认真核对各项服务内容完成情况；

2.采购人组织专家验收组进行验收；

3.验收结果不符合合同约定的，通知中标人限期达到合同约定的要求。详见合同相关规定。

6.7 知识产权

本项目实施完成新产生的所有技术成果的所有知识产权（包括但不限于著作权、专利权、商标权、专有技术等权利）的所有权、使用权、转让权以及收益等一切权利由采购人享有，本项目实施完成的发明创造的专利申请权、非专利技术的使用权、转让权归采购人享有。

附件三：本项目主要人员汇总表

乙方驻场人员如发生变更时需向甲方提交书面人员变更申请，经甲方项目负责人签字同意后方可进行人员变更。

序号	姓名	岗位	分工	电话
1	汪慧	项目经理	项目经理	13910837985
2	王巧雷	技术专家	技术专家	18601026243
3	王会雷	驻场服务工程师	驻场服务工程师	18601134363
4	肖厚新	驻场服务工程师	驻场服务工程师	13601367384
5	陈霞	服务工程师	服务工程师	18610330023
6	王振生	服务工程师	服务工程师	13910659420
7	连婧	服务工程师	服务工程师	18201618336
8	张佳伟	服务工程师	服务工程师	13691142555
9	赵军	服务工程师	服务工程师	18600364491
10	崔浩然	服务工程师	服务工程师	18610023215

附件四：验收标准

本项目在服务完毕之日起 10 个工作日内，乙方要提供所有服务期内产生的纸质文档和电子文档,并向采购人提出最终验收申请，采购人组织项目验收工作。

验收的主要标准为:

1.满足采购服务要求的各项指标；

2.项目各项工作应交付的报告、服务、知识产权或成果符合项目预期；

3.项目文档齐全，项目管理过程合规，项目人员管理到位；

4.在规定时间内顺利通过专家验收评审。

验收流程:

1.采购人成立验收小组，根据合同条款认真核对各项服务内容完成情况；

2.采购人组织专家验收组进行验收；

3.验收结果不符合合同约定的，通知中标人限期达到合同约定的要求。详见合同相关规定。

附件五： 保密协议

保密协议

甲方：北京市数字农业农村促进中心

乙方：北京华胜天成科技股份有限公司

经邀请招投标确定由 北京华胜天成科技股份有限公司 负责信息系统运维类项目（网络安全保障服务项目）01包-安全保障服务采购项目工作，为保护国家秘密、工作秘密、商业秘密和内部信息的安全，根据《中华人民共和国保守国家秘密法》及有关保密法律法规的规定，经甲乙双方友好协商，签订协议如下：

一、保密范围

1. 甲方告知乙方的、包括但不限于有关甲方或甲方管理服务对象的各种信息和甲方负有保密义务的各种信息，以及含有前述信息的各种纸介质、电磁介质、光盘介质的文件、资料，不论是否标有“绝密”、“机密”、“秘密”、“内部”、“保密”或类似字样。

2. 乙方在与甲方合作过程中产生的各种信息，或乙方以其他方式所知悉的有关甲方或甲方管理服务对象的各种信息、甲方负有保密义务的各种信息、以及含有前述信息的各种纸介质、电磁介质、光盘介质的文件、资料，不论是否标有“绝密”、“机密”、“秘密”、“内部”、“保密”或类似字样。

3. 根据合理的判断应理解为保密资料的，合理的判断是指如果此种秘密为本合同外的第三方知晓，能够使甲方遭受政治、经济损失或者丧失某种优势。

二、保密责任

1. 乙方应严格遵守《中华人民共和国保守国家秘密法》及有关保密法律法规的规定，对本协议规定的保密范围内的信息、资料等承担保密责任。

2. 乙方应加强对本方人员的保密管理。为此，双方同意：

①乙方应指定涉密人员参与涉密项目，并采取有效措施，保证其他无关人员不能接触到保密范围内的信息和数据。

（乙方为非保密资质单位的使用以下条款：乙方应对参与该项目的工作人员进行政治和背景审查，确保人员可靠。同时应采取有效措施，保证其他无关人员不能接触到保密范围内的信息和数据。）

②乙方应与本方人员签订保密协议，加强保密教育培训，对其行为进行监督和检查。

③乙方人员应严格遵守甲方的各项规章制度和保密要求，使用符合保密要求的SHEM计算机等设备处理保密范围内的相关信息。

④乙方工作人员不得将个人计算机、存储设备等带入甲方场所。

⑤乙方及乙方工作人员，不得擅自将保密范围内的信息和数据泄漏、告知、公布、发布、

出版、传授、复制、转让给第三方。

3. 乙方应采取有效措施，妥善保管保密范围内的信息和数据，防止丢失、被盗和扩散。在工作任务完成后，乙方应按照甲方要求，退回或销毁相关的保密资料，并对处理过相关信息的硬件设备进行信息消除处理，确保信息不被技术恢复。

4. 甲方要求乙方返还或销毁保密范围内的信息、数据及其复制件，乙方应予以执行，且不得私自留存。

5. 工作任务完成后，乙方及乙方工作人员仍应对其在完成工作任务期间接触、知悉的属于保密范围内的信息和数据履行保密义务。若发生泄密事件后，应积极配合甲方查找泄密原因，搜集线索和证据，并承担相应法律责任。

6. 甲方有权对乙方执行本协议和相关保密规定情况进行检查，乙方应予以配合，对检查中发现的问题应积极整改。

三、保密期限

协议自双方签字盖章之日起生效。除另有约定外，本协议项下的保密责任在本项目履行期间和本项目完成之后继续有效。

四、违约责任

乙方如违反本协议规定，应承担相应的法律责任和赔偿责任。

五、争议的解决

甲乙双方应通过友好协商解决因本保密协议产生的争议。协商不成，双方同意依法向北京市相关法院起诉。

六、其他

本协议一式柒份，甲方执肆份，乙方执叁份，自双方授权代表签字盖章之日起生效。

甲方：北京市数字农业农村促进中心
（盖章）

法定代表人或授权代表人：
（签字）：

签订日期：2026年 6月 8日

乙方：北京华胜天成科技股份有限公司
（盖章）

法定代表人或授权代表人
（签字）：

签订日期：2026年 6月 8日