合同编号：BCC-05-T-2023-07-14-018196

政府采购合同

项目名称：市科研院信息化安全运维服务项目

甲　　方：北京市科学技术研究院

乙　　方：北京市计算中心有限公司

合同协议书

本合同于2023年7月8日由北京市科学技术研究院(以下简称“甲方”)为一方和北京市计算中心有限公司(以下简称“乙方”)为另一方按下述条款和条件签署。

鉴于甲方为获得以下服务，即（市科研院信息化安全运维服务项目）而公开招标，并接受了乙方以总金额（人民币贰佰玖拾柒万元整¥2,970,000.00元）(以下简称“合同价”)提供上述服务的投标。

本合同在此声明如下：

1. 本合同中的词语和术语的含义与合同条款中定义的相同。

2. 下述文件是本合同的一部分，并与本合同协议书一起阅读和解释：

1）合同通用条款：

2）合同专用条款；

3）合同附件，如有：

附件1—中标通知书

附件2—服务内容

附件3—分项报价表

3. 考虑到甲方将按照本合同向乙方支付，乙方在此保证全部按照合同的规定向甲方提供服务。

4. 考虑到乙方提供的服务，甲方在此保证按照合同规定的时间和方式向乙方支付合同价或其他按合同规定应支付的金额。

第一节 合同通用条款

1. 定义

本合同中的下列术语应解释为：

（1）“合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和构成合同的所有文件。

（2）“合同价”系指根据合同规定，乙方在完全履行合同义务后甲方应支付给乙方的价格。

（3）“服务”系指根据合同规定乙方承担与运行维护有关的服务，如机房值守、设备维保、提供技术支持、培训和其他类似的义务。

（4）“工程实施”系指乙方根据合同规定须向甲方提供的、与服务相关的配置、部署等。

2. 技术规格

2.1 乙方提供和交付的服务项应与招标文件规定的技术规格以及所附的技术规格响应表（如果有的话）相一致。

3. 专利权

3.1 乙方应保证甲方在使用该服务或其任何一部分时不受第三方提出侵犯其专利权、商标权和设计权的起诉。

4.支付

4.1 本合同以人民币付款。

4.2 乙方应按照双方签订的合同规定提供服务。甲方按照《合同专用条款》规定的形式审核后付款。

5.技术资料

5.1 所有的技术资料，应于产品验收时一并交给甲方。

6.索赔

6.1 根据招标文件有关技术规格和要求向乙方提出索赔。

6.2 根据合同第 8 条和第 9 条规定的服务期内，如果乙方对甲方提出的索

赔和差异负有责任，乙方应按照甲方同意的方式解决索赔事宜。

6.3 如果在甲方发出索赔通知后 20 日内，乙方未作答复，上述索赔应视为已被乙方接受，如乙方未能在甲方提出索赔通知后 20 日内或甲方同意的更长时间内，按照本合同第 10.2 条规定的任何一种方法解决索赔事宜，甲方将从乙方开具的履约保证金中扣回索赔金额。

7.延迟提供服务

7.1 乙方应按照其在投标书中承诺的服务日期提供服务。

7.2 如果乙方因不可抗力以外的原因而拖延提供服务，将受到以下制裁：加收罚款和/或终止合同，按合同第 8.1 条规定执行。

7.3 在履行合同过程中，如果乙方遇到不能按时提供服务的情况，应及时以书面形式将不能按时交付使用的理由、延误时间通知甲方。甲方在收到乙方通知后，有权对情况进行分析，决定是否修改合同、酌情延长服务时间或终止合同。

8．违约罚款

8.1 除合同第 9 条规定外，如果乙方没有按照规定的时间给甲方和提供服务，甲方将处以罚款，罚款应从合同款中扣除，每延迟一周按 0.5%合同价计收罚款。但罚款的最高限额为合同价的 5%。一周按 7 日计算，不足 7 日按一周计算。如果达到最高限额，甲方可随时终止合同。

8.2 乙方违反本合同约定，提供本项目各服务不符合甲方要求的，由乙方负责根据甲方要求更正和修改，因此造成的所有损失和费用的增加由乙方承担。因此造成逾期交付的，乙方按照本合同 8.1 条承担逾期违约责任。

8.3 因乙方原因侵犯第三方合法权益造成甲方被卷入纠纷的，应由乙方承担全部责任，并至少应向甲方支付相当于合同总价款【5】%的违约金。因此给甲方造成的任何损失，乙方应承担赔偿责任，该损失包括但不限于诉讼费、仲裁费、律师费、调查费、第三方主张的赔偿金以及其他因此支付的合理开支。同时，甲方还有权解除本合同，乙方应退还甲方已支付的全部款项。在甲方因乙方原因卷入纠纷时，甲方有权自行决定聘请律师维护甲方的权益，但因此所发生的相关费用，均由乙方承担。

9．不可抗力

9.1 如果双方任何一方由于经双方同意属于不可抗力的事故，致使影响合同履行时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。

9.2 受事故影响的一方应在不可抗力发生后尽快以传真、电报、邮件通知另一方，并在事故发生后 14 日内，将有关部门出具的证明文件用挂号信寄给另一方。如果不可抗力影响时间延续 120 日以上时，双方应通过友好协商在合理的时间内达成进一步履行合同的协议。

10．税费

10.1 中国政府根据现行税法对乙方征收的与本合同有关的一切税费均由乙方负担。

11．履约保证金

11.1 乙方应在签订本合同后向甲方提供《合同专用条款》规定的履约保证金金额，履约保证金的有效期到服务保证期结束为止。

11.2 如乙方未能履行其合同规定的任何义务，甲方有权从履约保证金中取得补偿。

12．仲裁

12.1 在执行本合同中所发生的或与本合同有关的一切争端，甲乙双方应通过友好协商解决。如从协商开始 60 日内仍不能解决，双方应将争端提交有关市政府或行业主管部门寻求可能解决的办法。如果提交有关市政府或行业主管部门仍得不到解决，则应申请仲裁。

12.2 仲裁应向【北京仲裁委员会】按照该会现行仲裁规则进行仲裁。仲裁地在北京。

12.3 仲裁裁决应为终局裁决，对双方均有约束力。

12.4 在仲裁期间，本合同应继续执行。

13. 违约终止合同

13.1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可向乙方发出终止部分或全部合同的书面通知书。

(1) 如果乙方未能按合同规定的期限或甲方同意延长的限期内提供服务;

(2) 乙方在收到甲方发出的违约通知后20日内，或经甲方书面认可延长的时间内未能纠正其过失;

(3) 如果乙方未能履行合同规定的其它任何义务。

14.破产终止合同

如果乙方破产或无清偿能力时，甲方可在任何时候以书面形式通知乙方终止合同，终止该合同将不损害或影响甲方已经采取或将要采取的补救措施的权利。

15.转让

除甲方事先书面同意外，乙方不得部分转让或全部转让其应履行的合同义务。

16.适用法律

本合同应按中华人民共和国的法律进行解释。

17.合同生效及其它

17.1 合同在甲乙双方法定代表人或授权代表签字并加盖公章后即开始生效。

17.2 如需修改或补充合同内容，经协商，甲乙双方应签署书面修改或补充协议，该协议将作为本合同不可分割的一部分。

第二节 合同专用条款

合同专用条款是合同一般条款的补充和修改。如果两者之间有抵触，应以专用条款为准。合同专用条款的序号将与合同一般条款序号相对应。

1.定义

甲方：本合同甲方系指：北京市科学技术研究院

法人代表：伍建民

联系人：高远心　　联系方式：010-68731266-8249

乙方：本合同乙方系指：北京市计算中心有限公司

法人代表：刘彤

联系人：魏鹏　　联系方式：010-59341806

现场：本合同项下的服务提供地点位于：甲方指定地点

2.服务方式

2.1 本合同项下的服务方式为：参照本合同“附件二服务内容”。

2.2 乙方保证其交付给甲方的工作成果或服务不侵犯任何第三人的合法权益,并保证甲方免受第三方提出的索赔或诉讼。如因此发生第三人指控，乙方应当采取一切措施维护甲方的权益，以使甲方免于承担因此而引起的任何责任；由此产生的一切法律责任和经济责任（包括但不限于对第三人的责任以及由此导致甲方遭受的任何损失、索赔、支出的法律费用等）均由乙方承担。

3.付款条件

合同总额为人民币贰佰玖拾柒万元整¥（2,970,000.00 元），签订合同后 30 日内，乙方向甲方提交合同总价 3%的履约保函，提交履约保函后 30 日内，乙方开具有效发票后，甲方向乙方支付合同首款，即人民币贰佰零柒万玖仟元整（¥2,079,000.00 元）；2023 年 11 月底乙方提供 2 次运维服务报告（全年不少于 4 次运维服务报告）和有效发票并经甲方确认后 30 日内，甲方向乙方支付合同尾款，即人民币捌拾玖万壹仟元整(¥891,000.00 元)。

甲方和乙方因本合同发生的一切费用均以人民币结算及支付。

双方结算时，如遇财政国库结算等特殊时期，最终付款按照财政部门有关规定执行，不视为甲方违约。

4.检验和验收：

4.1 服务期结束后,甲方组织项目验收,并制作验收备忘录,签署验收意见。

5.索赔：

5.1 索赔通知期限：30 天。

6.不可抗力：

6.1 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后 30 天内，将有关部门出具的证明文件送达另一方。

6.2 不可抗力使合同的某些内容有变更必要的，双方应通过协商在30天内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

7.履约保证金：

7.1 提交履约保证金的时间：签订合同后30日内

履约保证金金额：合同总价的3%，即人民币捌万玖仟壹佰元整（¥89,100.00元）

履约保证金形式：履约保函

8.合同生效和其它

8.1 本合同经双方法定代表人或授权代表签字并加盖公章后生效。

8.2 本合同一式捌份，以中文书写，甲方执肆份，乙方持贰份，壹份报北京市市政府采购办公室备案，壹份递交招标代理机构备案，具有同等法律效力。

8.3 如需修改或补充本合同内容，经协商，双方应签署书面修改或补充合同，该合同将作为本合同的一个组成部分。

8.4 乙方同意甲方在北京市政府采购网站上公布乙方联系方式、服务收费标准及服务承诺情况。

8.5 乙方接受甲方及北京市政府采购监督部门不定期的监督检查。

9. 合同有效期

本合同有效期自2023年7月8日起至2024年7月7日止。

（以下无正文）

甲方：北京市科学技术研究院

（盖章）

法定代表人或授权代表签章：

签订时间：2023年7月25日

乙方：北京市计算中心有限公司

（盖章）

法定代表人或授权代表签章：

签订时间：2023年7月25日

附件一、中标通知书

BWTC

北京国际贸易有限公司

BEIJING WORLD TRADE CORPORATION

中国北京建国门外大街甲3号 邮编：100020

A-3 JIANGUOMEN WAI STREET,BEIJING 100020 CHINA TEL:86-10-85343310

中标通知书

北京市计算中心有限公司：

在我公司组织的市科研院信息化安全运维服务项目(招标编号：0686-2311BE1224012)中，经评标委员会评审后，确定贵公司为本项目的中标单位，中标金额为：￥2,970,000.00(人民币贰佰玖拾柒万元整)。

请贵公司在中标通知书发出之日起30日内，按照招标文件确定的事项与采购人签订政府采购合同，并在合同签订之日起2个工作日内将合同原件扫描件发至招标文件中指定邮箱。

特此通知。

北京国际贸易有限公司

2023年7月7日

附件二、服务内容

1. 项目概述

2023年，市科研院需要信息化安全运维服务，利用第三方专业安全力量，持续提升市科研院风险抵御能力、化解安全压力，对现有安全能力进行补充和优化，缩短各类安全事件处理响应和分析时间，有效保障市科研院的网络安全及业务系统持续正常运行，并针对服务范围内资产进行持续风险监视，同时提供远程值守团队进行安全保障，提升用户运营效率，更好的支撑市科研院“十四五”创新发展规划，为市科研院科技创新工作的开展起到了关键作用。

市科研院信息化安全运维服务包括安全运维服务、安全认证服务和安全监控及响应服务三个部分。

2. 服务内容

2.1. 安全运维服务

安全运维服务包含了安全巡检服务、安全风险评估服务、安全加固服务、安全设备质保和特征库升级服务。

2.2.1. 服务期限

自合同签订之日起1年

运维保障时段：

安全巡检服务，安全风险评估服务，安全加固服务：工作日早9:00-晚17:30。

安全设备质保服务：7*24*8（7天24小时，8小时内响应解决）。

2.2.2. 安全巡检服务

提供甲方业务系统的主机和57台安全设备日常巡检和维护、故障排除、节点周期性检查，发现潜在问题，提供解决建议。每年重大会议、活动、节日期间的7*24小时的技术支持保障服务。

在安全巡检服务中，通过制定详细的巡检服务计划及巡检服务流程，并完善巡检内容，提供符合甲方要求的安全巡检服务。

对甲方安全系统进行全面检查，获得系统运行的第一手资料，最大可能地发现存在的隐患，保障安全系统稳定运行。同时，针对性地提出预警及解决建议，

使甲方能够提早预防，最大限度降低运营风险。

提供 1 年 5*8 小时驻场工程师 1 名。

2.2.3. 安全风险评估服务

提供北科院业务系统和网络安全设备的风险评估和漏洞扫描服务，定期提供扫描报告和风险解决建议。

风险评估需要评估和分析网络上存在的技术和管理风险；梳理业务访问关联关系，分析业务运作和管理方面存在的安全缺陷；调查信息系统的现有安全控制措施，评价业务安全风险承担能力；评价风险的优先等级，据此提出风险控制措施建议。

针对漏洞和风险管理，需要通过漏洞扫描系统对发现的系统安全漏洞进行及时修补；需要定期安装最新补丁程序，对重要漏洞进行及时修补；定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

提供 1 年 5*8 小时驻场工程师 1 名。

2.2.4. 安全加固服务

安全加固服务提供北科院业务系统的主机安全防护服务和主机加固服务。

主机操作系统安全加固不仅能够实现基于文件自主访问控制，对服务器上的敏感数据设置访问权限，禁止非授权访问行为，保护服务器资源安全；更是能够实现文件强制访问控制，即提供操作系统访问控制权限以外的高强度的强制访问控制机制，对主客体设置安全标记，授权主体用户或进程对客体的操作权限，有效杜绝重要数据被非法篡改、删除等情况的发生，确保服务器重要数据完整性不被破坏。

主机安全防护服务和主机加固服务包括操作系统安全加固、关闭不必要的服务、端口、共享和来宾组等，为不同用户开放相应权限，防止安装不必要的应用软件；对终端外设接口、外联设备及使用的监视、有效控制计算机的资源利用率；实现系统密码口令安全策略管控、系统资源文件使用访问控制、主机基础资源使用监控等安全功能。

提供 1 年 5*8 小时驻场工程师 1 名。

2.2.5. 安全设备质保

对运行在内网系统的 57 台安全设备提供 1 年的设备保修服务，签订合同后

1 年内所有非人为出现的硬件故障，由乙方负责解决。提供服务期内的备件更换服务，第一时间利用现场备件库的备件进行更换，如果现场无备件，工程师报服务台申请备件，备件 2 小时内送达甲方现场进行更换。所更换的备件均为原厂备件，且与原设备或模块型号相同，各项性能规格不低于原有设备。并且所提供的备件自更换之日起一年保修。质保设备清单如下：

序号	型号	数量	运行地点
1	迪普 FW1000-GA-E	1	首创金融中心负一层
2	迪普 WAF3000-ME	1	首创金融中心负一层
3	迪普 IPS2000-ME-N	1	首创金融中心负一层
4	迪普 IPS2000-ME-N	1	首创金融中心负一层
5	迪普 UAG3000-ME	1	首创金融中心负一层
6	迪普 UAG3000-ME	1	首创金融中心负一层
7	迪普 DPX8000-A5	1	首创金融中心负一层
8	天融信 IDP3000 TI-6130-DDOS	1	首创金融中心负一层
9	天融信 IDP3000 TI-6130-DDOS	1	首创金融中心负一层
10	天融信 TOPSENTRY3000	1	首创金融中心负一层
11	天融信 TOPFILTER8000 TF-2604	1	首创金融中心负一层
12	天融信 TOPFILTER8000 TF-2604	1	首创金融中心负一层
13	天融信 TA-6214-DB	1	首创金融中心负一层
14	迪普 FW1000-TS-A	1	首创金融中心负一层
15	迪普 WAF3000-TS-A	1	首创金融中心负一层
16	锐捷 RG-OAS1000E	1	首创金融中心负一层
17	中安星云 DF3000-T-A	1	首创金融中心负一层
18	CA 认证网关	1	首创金融中心负一层
20	深信服 VPN 1000E	1	首创金融中心负一层
22	防火墙天融信 NGFW4000	1	数字经济所
23	深信服 ADBJ-110	1	数字经济所
24	蓝盾 BD-VPBJ-210 防火墙	1	数字经济所
25	蓝盾 BD-VPBJ-215 防火墙	1	数字经济所

26	蓝盾 BD-VPBJ-210 防火墙	1	数字经济所
27	深信服 STA-100B440	1	数字经济所
28	深信服 SIP-1000-B400	1	数字经济所
29	奇安信 网神 SecVSS 3600	1	数字经济所
30	蓝盾 BD-VPBJ-445 数据库审计	1	数字经济所
31	建恒信安 JH-OAM-TG1000 堡垒机	1	数字经济所
32	深信服 ADBJ-110	1	数字经济所
33	深信服 VPBJ-110	1	战略所
34	任子行防火墙	1	战略所
35	Webray 漏洞扫描	1	战略所
36	Webray 网页防篡改	1	战略所
37	Webrayweb 防火墙	1	战略所
38	Ngfre WALL 400	1	城市系统工程研究所
39	NI3100-60	1	城市系统工程研究所
40	深信服 AF 1000	1	智能装备研究所
41	SG6000-M3662	1	北科大厦
42	allot AC804	1	北科大厦
43	pa-410	1	北科大厦
44	ASA5510-K8	1	北科大厦
45	无线安全网关	1	北科大厦
46	网风险可视化追溯防火墙	1	北科大厦
47	网络故障自愈网关 iRecovery1000	1	北科大厦
48	流量控制 Acenet AG1200	1	北科大厦
49	病毒网关 PAN-PA-500	1	北科大厦
50	行为管理网康 NI3310	1	北科大厦
51	McAfee EmailGatewayEG5000 Appliance 网关	1	北科大厦
52	趋势客户端病毒防护	1	北科大厦
53	macafee 服务器端病毒防护	1	北科大厦

54	深信服 AD 1900	1	情报所
55	深信服 AF 1580	1	情报所
56	深信服 AC 1750	1	情报所
57	深信服 AF 1520	1	情报所
	合计	57	

2.1.5.1. 服务标准

编号	衡量项目	服务内容	服务标准
1	故障及时响应并处理	故障解决率≥95%，每月	一级故障四小时内解决 二级故障三小时内解决 三级故障二小时内解决 四级故障一小时内解决
		重大故障次数≤4 次	全年重大故障即四级故障次数小于等于 4 次

提供网络设备维保、安全设备维保、存储设备维保、服务器设备维保、VPN 设备维保、虚拟化软件更新和升级、配件保障等，保障各种设备的正常运行。

2.1.5.2. 服务内容

1）故障解决服务

乙方接到甲方提出的故障处理请求后，在规定的响应时间内对指定 IT 设备、故障进行响应，分析、明确故障发生原因，并在规定的恢复时间内恢复设备的正常运行，必要时恢复相应数据。

乙方提供的故障处理服务包括但不限于：

1．故障定位；

2．确定、分析故障原因；

3．根据故障等级（参见下表）采取措施，防止故障影响范围进一步扩大；

4．对于短期内无法解决的故障，提出并执行替代方案；

5．提出并执行故障解决方案；

6．对于重大故障，协调、召集相关技术专家论证故障解决方案；

7．必要时恢复设备的操作系统、软件配置和数据等；

8．对于 IT 设备应更换损坏的设备部件或整机，安装、调试新的设备部件或整机；

9．总结故障处理过程，提出相关改善建议，防止类似故障再次发生。

2）备件服务

乙方具有设施完整、规模较大、管理完善的本地备件储备库。

为甲方提供备件支持，合同签订后，乙方根据备件服务设备清单，准备相应规格相应数量的备件，在甲方设备出现故障需更换备件时，为甲方替换备件。乙方针对本项目中的设备情况提供充足的备品备件，且提供的备件均是原厂备件，不以其它方式替代。

甲方有权随时对备品备件库存情况进行现场查验，一经发现库存情况与服务提供商承诺不符，甲方将有权取消与乙方合作资格。

当应用系统主机设备出现致命性的严重故障而无法及时修复时，乙方的现场工程师将采用现场备件来顶替出故障的主机，以保证应用系统恢复的时效性，主要包括硬盘、内存、电源等易损部件。乙方在投标文件中详细说明日常备件保障及支持体系，并制定备品备件详细的部署方案。

乙方具有设施完整、规模较大、管理完善的本地备件储备库，备件库的种类应覆盖设备清单中的设备类型.

（1）主机系统硬件保养

为保障设备的正常使用和延长其工作寿命，乙方专业技术人员针对主机硬件每季度给予清洗除尘维保，保持硬件的清洁，降低硬件故障发生概率，提高系统的可靠性。

（2）性能分析及系统调优

在甲方维保服务范围内的设备性能下降及时找出瓶颈，乙方提供相关的建议，制订出性能调优方案，在甲方批准后付诸实施。及时消除系统隐患，避免造成业务中断；在不增加或少增加投资的同时，提高系统的运行性能和可管理性。

（3）主机系统集群审核

集群系统主要用于关键业务，乙方对甲方系统进行集群审核，以确保高可用

性，集群在故障发生时能正常切换。

（4）服务质量管理要求

乙方根据本项目要求，提出服务质量管理及监控具体措施，并对所提供的服务质量和标准做出明确可量化的承诺，对不能达到服务承诺和标准的情况制定相应的赔偿条款。

3）软件升级服务

在不影响现有业务系统正常运行的前提下：

1. 对服务范围内设备的软件在必要的时候进行版本升级；
2. 对系统设备软件进行必要的补丁升级、漏洞修补。

4）保养

（1）主机系统硬件保养

为保障设备的正常使用和延长其工作寿命，乙方专业技术人员针对主机硬件每季度给予清洗除尘维保，保持硬件的清洁，降低硬件故障发生概率，提高系统的可靠性。

（2）性能分析及系统调优

在甲方维保服务范围内的设备性能下降及时找出瓶颈，乙方提供相关的建议，制订出性能调优方案，在甲方批准后付诸实施。及时消除系统隐患，避免造成业务中断；在不增加或少增加投资的同时，提高系统的运行性能和可管理性。

（3）主机系统审核

系统主要用于关键业务，乙方对甲方系统进行集群审核，以确保高可用性，在故障发生时能正常切换。

（4）服务质量管理要求

乙方根据本项目要求，提出服务质量管理及监控具体措施，并对所提供的服务质量和标准做出明确可量化的承诺，对不能达到服务承诺和标准的情况制定相应的赔偿条款。

5）重点保障服务

乙方在国家重要安全保障周期提供重点保障服务，增派满足数量和技能要求的现场运维人员和必要的后台支持运维人员，进行 24 小时值守。

6）后备技术支持服务

乙方除按甲方要求提供驻场运维工程师外，还为甲方成立专门后备技术专家

和管理专家团队，负责重大事件现场处理和运维项目的有效运维管理。

2.2.6. 特征库升级

对运行在内网系统57台安全设备中的30台安全设备提供1年的数据库、特征库、病毒库升级服务。软件及特征库升级至当前最新版本并技术支持1年。设备清单如下：

序号	型号	数量	运行地点
1	迪普 FW1000-GA-E	1	首创金融中心负一层
2	迪普 WAF3000-ME	1	首创金融中心负一层
3	迪普 IPS2000-ME-N	1	首创金融中心负一层
4	迪普 UAG3000-ME	1	首创金融中心负一层
5	迪普 DPX8000-A5	1	首创金融中心负一层
6	天融信 TOPFILTER8000 TF-2604	1	首创金融中心负一层
7	迪普 FW1000-TS-A	1	首创金融中心负一层
8	迪普 WAF3000-TS-A	1	首创金融中心负一层
9	中安星云 DF3000-T-A	1	首创金融中心负一层
10	深信服 ADBJ-110	1	数字经济所
11	蓝盾 BD-VPBJ-210 防火墙	1	数字经济所
12	蓝盾 BD-VPBJ-215 防火墙	1	数字经济所
13	蓝盾 BD-VPBJ-210 防火墙	1	数字经济所
14	深信服 SIP-1000-B400	1	数字经济所
15	奇安信 网神 SecVSS 3600	1	数字经济所
16	深信服 VPBJ-110	1	战略所
17	任子行防火墙	1	战略所
18	Webray 漏洞扫描	1	战略所
19	Webray 网页防篡改	1	战略所
20	Webrayweb 防火墙（串行）	1	战略所
21	Ngfre WALL 400	1	城市系统工程研究所
22	深信服 AF 1000	1	智能装备研究所
23	流量控制 Acenet AG1200	1	北科大厦

24	病毒网关 PAN-PA-500	1	北科大厦
25	行为管理网康 NI3310	1	北科大厦
26	McAfee EmailGatewayEG5000 Appliance 网关	1	北科大厦
27	深信服 AD 1900	1	情报所
28	深信服 AF 1580	1	情报所
29	深信服 AC 1750	1	情报所
30	深信服 AF 1520	1	情报所
	合计	30	

2.2. 安全认证服务

2.2.1. 服务期限

自合同签订之日起 1 年

运维保障时段： 7*24*8（7 天 24 小时，8 小时内响应解决）。

2.2.2. 服务内容

名称	内容
服务范围	统一身份认证升级维护服务。 短信认证运维服务 短信平台维护服务
总体目标	保障每个用户在各个应用系统上分配统一的用户名和密码，建立统一登录界面，从而简化业务用户访问应用系统的行为，提升业务用户访问应用系统的效率和便捷性。统一用户账号管理，实现用户及密码的集中管理，从而实现对应用系统用户的集中管理，大大提升用户管理能力。 具体目标如下： ➢ 保障软件的稳定性和可靠性； ➢ 保障软件的安全性和可恢复性； ➢ 故障的及时响应与修复；

	➢ 软件设备的维护服务； ➢ 硬件设备的维护与指导应用； ➢ 保障短信平台短信验证稳定性和可靠性
服务内容	统一身份认证： 组织架构梳理，对接新增业务系统，要求服务方提供对接端口，满足与现有系统数据对接，实现用户及组织机构数据统一管理。 平台数据迁移，数据对内部用户的入离调转等数据变更能够与 HR 系统保持同步，外部用户可通过统一身份认证系统手动维护。业务系统用户及组织机构数据由统一身份认证系统集中供给，实现各业务系统组织机构的统一管理，方便业务系统内账号实体人员的信息维护。
	乙方根据系统情况提供对接方案，并实现以下列出的对接服务效果，其提供的对接服务应实现包括但不仅限于以下内容。 应用系统对接服务：实现新增业务系统应用的对接统一管控及单点登录 SSO 更新。 安全网关对接服务：实现新增业务系统应用访问结合安全网关，对用户访问应用时，提供反向代理，逻辑隔离，安全认证，保证应用系统的安全访问。 用户授权：新增业务系统应用对接服务应满足新增业务系统不低于 500 用户注册，提供 500 用户认证服务授权； 对接调优：针对对接服后的应用情况进行调优，结合应用存在或潜在的问题，并及时提交对接后系统性能优化调整建议方案，保证系统的高效运行。 如对接后应用出现故障，导致系统不能正常工作，技术人员会尽快解决问题并保证问题完全解决。
	入网认证平台服务 技术支持(人工客服：7×24,官网智能机器人客服：7×24；远程问题处理(5×8)； 在线技术支持(产品技术资料和主机软件补丁下载)；

		软件更新支持(提供主机版本软件的维护版本) 备件先行服务（5x8（周一至周日，00:00～24:00，到达：4 小时内到达，备注：特殊原因如设备所在地不在覆盖城市范围内或者设备所在地距离最近的备件库 50 公里以上，亦或者特殊天气或者交通状况原因，备件达到时间可能适当延长） 设备健康检查，每年四次对维保设备进行巡检。检查设备运行状况，并针对性地提出预警及解决建议，使用户能够提早预防，最大限度降低运营风险；（每季度上门维护 1 次）
		短信平台维护服务 满足入网用户接收验证码，10 万条/一年
服务方式		对系统提供对接服务，并提供相应的对接设计方案。乙方为对接服务后的功能及效果提供一年的保障。

2.3. 安全监控及响应服务

2.2.1. 服务期限

自合同签订之日起 1 年。

运维保障时段： 7*24*8（7 天 24 小时，8 小时内响应解决）。

服务厂商：由第三方专业安全厂商（奇安信网神信息技术(北京）股份有限公司）提供安全服务。

2.2.2. 服务内容

序号	服务内容	指标项	招标要求
1	首次运营评估	首次资产梳理	提供使用人工梳理的方式整理市科研院资产信息，同步到安全运营指挥中心云端安全运营平台；
2		首次威胁分析	服务团队能够通过部署在客户侧的服务工具对市科研院流量进行分析，包括 APT 告警分析、恶意软件情况分析、网络攻击情况分析、WebShell 情况分析、内网安全情况分析、数据库安全情况分析、爆破行为分析、弱口令分析等，输出首次分析报告。
3	资产管理	设备管理	为保障服务工具正常运转，服务人员对服务工具 CPU、存

		和维护	储情况、系统时间、授权、功能模块等巡检，避免故障影响服务工具正常运行。为保障威胁检测能力，服务人员对服务工具威胁情报版本和更新状态进行检查和升级。日常巡检发现服务工具故障后，服务人员协调跟踪产品售后人员对服务工具进行故障修复。
4		支持查看网站资产详情	可自动获取网站备案信息，包含以下信息： 备案信息：网站备案号 、网站名称 、网站首页地址、审核日期 、注册信息 注册信息：注册商 、域名服务器、责任人姓名、责任人邮箱、责任人电话 安全告警统计：各类型告警数量统计 网站 IP 地址列表展示、网站 DNS 列表展示
5		支持网站目录结构展示	支持展示网站目录结构，以树形模式展示
6		资产管理	支持对于本单位所负责运营的资产，允许进行资产的新建、编辑以及删除工作；支持单个资产及批量资产添加
7		资产识别	服务人员每季度提供对市科研院资产台帐进行检查，补充完善资产变更情况。支持根据添加资产的域名/ip 发现未知资产。
8			支持最近一周告警趋势、已知资产/未知资产统计、未处理高危告警 TOP5、各告警类型数量统计
9	漏洞管理	扫描深度	每日扫描网站一万个以上，扫描深度最高可达 9999
10		漏洞发现及处置	支持针对常见漏洞进行程序自动化验证，并可将自动验证漏洞生成安全告警
11			支持三种漏洞验证方式如浏览器验证、注入验证、通用验证；
12			支持同时下发系统扫描、Web 扫描、弱口令扫描任务，无需单独下发扫描任务，扫描目标可以是 IP、域名、URL 的

			任一格式；
13			支持根据攻击载荷自定义漏洞检测规则，可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）、匹配载荷内容，并且单条规则可指定多个检查项，同时可定义漏洞威胁级别、威胁分类、攻击结果、CVE 编号、CNNVD 编号、漏洞描述、漏洞危害、解决方案；
14			支持展示资产漏洞信息，信息包括：资产 IP、资产名称、资产组、漏洞名称、最近发现时间、威胁级别、漏洞来源、漏洞披露时间、CVE 编号、CNNVD 编号。并支持导入漏洞知识库文件；
15			支持配置展示云端平台漏洞情报及资产漏洞信息；
16	安全威胁监测	服务频率	服务团队通过云端安全运营平台提供 7*24 安全威胁监测服务，持续监测网络内的安全隐患情况并进行分析，包括对外部网络攻击网络漏洞利用情况、恶意软件活动情况、以及内网安全情况。普通资产事件发生 12 小时内完成告知，极速 SLA 响应资产按照服务等级协议承诺时间进行告知。
17		威胁情报	支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报。
18		云端联动	支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等
19	主动响应分析	安全分析	服务人员综合所发现的安全事件、攻击情况，评价客户侧整体网络安全态势，包括但不限于告警趋势分析、威胁类型分布分析、高威胁攻击者分析等。并在每月主动进行场景化安全分析，包括 APT 告警分析、恶意软件情况分析、网络攻击情况分析、WebShell 情况分析、内网安全情况分

			析、数据库安全情况分析、爆破行为分析、弱口令分析等。
20		非常规访问分析	支持可疑代理分析：能够发现 socks、http、reDuh、Regeory Tunnel、Tunna 等代理类型
21			支持远程工具分析：能够发现 pc_anywhere、ultra_vnc、chrome_remote_desktop、 oray、teamviewer 等远程工具类型
22			支持反弹 shell 分析：能够展示受害 IP、攻击 IP、端口、受害地域/资产组、攻击地域/资产组、最近访问时间等详细信息
23		登录行为分析	支持异常登录行为检测，检测内容包括：源 ip、账号、登录资产 IP、使用协议、登录结果等信息，且能进行异常时间配置，
24		特权账号分析	支持 ssh、telnet、ftp、smb 等常见协议特权账号登录行为分析，且能自定义特权账号
25		访问行为分析	支持外部访问分析，能展示源 ip、资产 ip、端口、协议、时间等详细信息，且能自定义源 ip 白名单
26		DNS 访问分析	支持可疑 DNS 解析：能够检测发现 DGA 域名与 DNS 隧道域名，支持根据时间范围、请求次数、DNS 域名总长度自定义 DNS 隧道检测规则
27	网站云监测	10 个域名一年网站云监测平台的使用权	提供 10 个域名一年网站云监测平台的使用权；并提供以下内容：漏洞扫描（最快频率 3 天）、违规内容监测（最快频率 2 小时）、网页挂马监测（最快频率 2 小时）、内容变更监测（最快频率 2 小时）、黑链监测（最快频率 2 小时）、网站可用性监测（最快频率 2 分钟）以及标准的报表管理和通报管理模块；不支持提供 API 接口，不支持定制。
28		售后要求	提供单个域名一年的基础人工运维服务，服务内容包括：7X24 小时的安全事件监测验证和安全事件通告下发； 定期远程漏洞扫描及高危漏洞人工验证； 7X24 小时电话售后服务

29		网站漏洞监测	对发现网站存在的 SQL 注入、XSS 跨站脚本、目录遍历、文件包含、备份文件、敏感文件等漏洞，检测内容覆盖 WASC 分类的多种 Web 应用漏洞和 OWASP TOP10 网站漏洞进行管理；定期跟踪漏洞的修复情况从而使网站的漏洞得以快速修复，降低网站被入侵的风险。 利用 POC 对目标网页进行 WEB 漏扫，发现 SQL 注入漏洞、命令注入、CRLF 注入、LDAP 注入、XSS 跨站脚本漏洞、路径遍历漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞、等安全漏洞问题 对 mysql、redis、ftp、ssh 等弱口令进行监测
30		网站黑链监测	使用模拟浏览器，爬虫 UA 等多种技术发现网站黑链，支持图片暗链的检测，支持全站对于潜藏在页面深处的第三方黄赌毒广告类链接进行监测并告警，可定位源代码黑链的位置和内容。黑词样本数 5700，2021 年检测黑链告警事件 629W，支持配置监测频率，支持任务并发量配置，支持用户自定义黑词。
31		违规内容监测	结合海量词库及人工识别，通过机器学习手段，提供敏感词发现的技术手段，支持全站监测，可定位敏感词位置和内容。涉及敏感词样本 10000，2021 年检测违规内容告警事件 600W，支持配置监测频率，支持任务并发量配置，支持用户自定义敏感词，支持网页附件内容检测。
32		内容变更（篡改）监测	首页及重点页面：页面发生变更即产生告警，变更类型包括外链、黑词、body 标签为空、HTML 之外内容。
33		安全监测频次	爬虫： 网站黑链监测：默认全站 120 分钟/次 违规内容监测：默认全站 120 分钟/次 内容变更监测：默认首页 120 分钟/次，支持对自定义 URL 监测

			网站挂马监测：默认首页 120 分钟/次 漏扫： 网站漏洞扫描：默认全站 7 天/次（可调整为 3 天、5 天、7 天、15 天、30 天） 可用性： 可用性监测：默认首页 2 分钟/次
34	应急响应	服务要求	配合威胁检测与响应服务（MSS-TDR）的 7*24H 实时监测，在市科研院发生确切的安全事件需要现场应急响应时，提供现场应急响应服务 4 次。
35	安全厂商服务资质	资质证书	具备国家计算机网络应急技术处理协调中心颁发的 CNCERT 应急服务支撑单位(APT 监测分析领域)资质证书
36		资质证书	具备中国通信企业协会颁发的中国通信企业协会通信网络安全服务能力评定证书-应急响应资质证书
37		资质证书	具备中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质-应急处理资质证书
38		资质证书	具备中国网络安全审查技术与认证中心颁发的 CCRC 信息安全服务资质-安全运维资质证书

附件三、分项报价表

序号	分项名称	单价（元）	合价（元）	备注/说明
1	安全运维服务	￥2,050,000.00	￥2,050,000.00	无
2	安全认证服务	￥380,000.00	￥380,000.00	无
3	安全监控及响应服务	￥540,000.00	￥540,000.00	无
总价（元）			￥2,970,000.00	/