Z-24-JGB-152

合同备案
BRTV
2025年1月7日

HT24-084

政府采购合同

项目名称：2025年度网络安全技术服务项目

甲方：北京广播电视台

乙方：奇安信网神信息技术（北京）股份有限公司

第一部分 合同书

鉴于：

北京广播电视台（甲方）所需“2025 年度网络安全技术服务项目”经北京国泰建中管理咨询有限公司以 11000024210200103023-XM001 号招标文件在国内公开招标。经评标委员会评定奇安信网神信息技术（北京）股份有限公司为乙方。甲方与乙方协商一致，依据《中华人民共和国民法典》、《中华人民共和国政府采购法》等有关法律、法规和规章的规定，根据《项目招标文件》（以下简称“招标文件”）中的相关规定，在自愿、平等、协商一致的基础上，同意按照下列条款，签订本合同。

1. 合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。且按如下顺序进行解释：

A. 本合同书

B. 合同条款及其附件

C. 中标通知书

D. 招标文件(含招标文件补充通知、澄清文件)

E. 投标文件(含澄清文件)

除非另有特殊约定，在本合同的履行过程中，对本合同未尽事宜的约定及对本合同的任何修改，均须由双方协商一致并签署书面补充协议方为有效。补充协议构成本合同的组成部分，其优先解释顺序应视其内容与其它合同组成部分的相互关系而定。

乙方须详细审阅全部合同文件。如乙方发现任何合同文件的组成部分之间有任何不一致或歧义时，应即时以书面形式向甲方指出不一致或歧义之处。甲方有权自行或依据乙方要求就不一致或歧义之处发出有关指令。该指令为最终决定，乙方应予遵守，并不得以遵照该指令为由向甲方索偿任何费用或要求延长验收时

间。

2. 技术服务

甲方委托乙方提供 2025 年度网络安全技术服务，包括安全规划服务、安全咨询服务、安全运维技术服务、渗透测试服务、重要时期保障服务、实战攻防演习支撑服务、应急演练与应急响应服务、红队评估服务、迎检专项服务、安全设备服务、终端防病毒服务、移动端安全加固服务、信息系统等保测评、容器安全检测服务以及蜜罐服务。本合同的具体服务内容及要求详见附件二《技术方案》。

3. 合同总价

本合同为固定总价合同，合同总价为人民币 2389500 元整（大写：贰佰叁拾捌万玖仟伍佰元整）。

此价格已包含技术服务费、相关软件开发费、保险费和调试费、售后服务费、综合费率、总利润、税金等过程中可能发生的一切费用。乙方不得向甲方再加收任何费用。具体见分项报价表。

4. 付款方式

本合同的付款方式：详见合同特殊条款。

5. 服务周期

本合同的服务周期：详见合同特殊条款。

6. 服务地点

本合同的服务地点：详见合同特殊条款。

7. 合同的生效

本合同自 2025 年 1 月 1 日起生效。

甲　方：北京广播电视台

法定代表人或

授权代表(签字)：

2025年1月26日

地　　址：北京市朝阳区建国路98号

电　　话：010-85335821

开户银行：工商银行北京建国路支行

账　　号：0200041909200678957

乙　方：奇安信网神信息技术（北京）股份有限公司

法定代表人或

授权代表(签字)：

2025年1月23日

地　　址：北京市西城区西直门外南路26号院1号楼2层

电　　话：010-57836300

开户银行：招商银行北京建国路支行

账　　号：110902261210404

第二部分 合同条款

1. 定义

1.1 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、附录和构成合同的其他文件。

2) “合同价”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的价格。

3) “软件”包括“软件系统”，除另有指明外，指在本合同履行期内所开发和提供的当前和将来的软件版本，包括乙方为履行本合同所开发和提供的软件版本和相关的文件。

4) “服务”系指根据本合同规定乙方承担与网络安全技术有关的招标文件要求的各项服务，该等技术服务的费用业已包含在合同价中。

5) “甲方”系指与中标人签署服务合同的人（含最终用户）。

6) “乙方”系指根据合同约定提供相关服务的中标人。

7) “现场”系指合同约定的地点。

8) “验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的服务符合合同规定的活动。

9) “商业秘密”指甲、乙方各自所拥有的，不为公众所知的管理信息、方式方法、顾客名单、商业数据、产品信息、销售渠道、技术诀窍、源代码、计算机文档等，或由甲、乙方在履行本合同过程中明确指明为商业秘密的、法律所认可的任何信息。

10) “工作日”指国家所规定的节假日之外的所有工作日，未指明为工作日的日期指自然顺延的日期。

2. 服务内容与要求

详见附件二《技术方案》。

3．技术规范及质量保证

3.1 乙方提供服务的技术规范应与招标文件规定的技术规范和技术规范附件(如果有的话)及其投标文件的技术规范偏差表(如果被甲方接受的话)相一致，若技术规范中无相应说明，则以国家有关部门最新颁布的相应标准及规范为准；若国家相关部门无相应标准，则以行业标准及规范为准。

如果在合同履行过程中有新的国家或行业（部）标准出台的，且该标准属于强制性标准的，则乙方应确保该合同产品达到并符合新的国家或行业（部）标准。因此而增加的费用及风险已经包含在合同总价中。

3.2 乙方保证其在本合同项下供应的全部服务技术水平是先进的、成熟的、质量优良的；所需使用的设备选型均符合安全可靠、经济运行、易于维护的要求并完全符合本合同的规定。乙方进一步保证其在本合同项下所交付的全部技术资料内容完整、统一、准确、有效，并能满足甲方需求。

4．承诺与保证

4.1 乙方保证

（1） 法人地位

乙方是一家根据中华人民共和国法律设立、合法存续的、合法经营并具有良好信誉的公司，具有合法的、完全的民事权利能力和行为能力签署和履行本合同项下的义务和具备我国相关法律规定的与甲方签署本合同的资质。

（2） 利益冲突

乙方签署和履行本合同或与本合同相关的文件将不会

A、与乙方的章程或其他适用于乙方的法律法规或判决相冲突；

B、与乙方同第三人所签署的任何法律文件如保证协议、承诺、合同等规定的义务相冲突或导致任何违约，或使乙方的权利受到

约束。

（3） 侵权与被诉

知识产权保证：乙方在此不可撤销地承诺，乙方为履行此合同，向甲方提供服务所需使用的软件及相关技术未侵犯任何第三人的知识产权，甲方（包括最终使用方）依据本合同及双方约定的其他文件对该技术包括但不限于使用、收益、处分的行为，不存在任何侵权可能和被任何第三方追究任何法律责任。

若甲方或最终用户因此受到了损失，该损失包括但不限于对第三方任何赔偿、补偿、垫付的款项以及应对指控而支出的全部费用，均由乙方承担。

乙方提供的服务若经政府部门或其他相关质量鉴定机构认定存在质量问题或安全隐患，导致今后使用过程中造成甲方或第三方人身伤亡或财产损失的，乙方承担由此产生的全部责任。如甲方因此遭受索赔，甲方有权向乙方追偿（追偿范围包括但不限于赔偿金、鉴定费、评估费、诉讼费、合理的律师费等）。

（4） 合法服务

乙方保证其使用的软件符合国家有关软件产品方面的规定和软件标准规范。

（3）乙方保证在所提供网络安全服务中，不含任何可以自动终止或妨碍系统运作的软件/程序/源代码。

（4） 合同条款中应规定， 乙方完全遵守《中华人民共和国妇女权益保障法》中关于“劳动 和社会保障权益”的有关要求。

4.2 甲方保证

（1）甲方具有合法的权利缔结本合同，具有合法的、完全的民事权利能力和行为能力来签署并履行本合同项下的义务。

（2）利益冲突

甲方签署和履行本合同或与本合同相关的文件将不会

A、与甲方的章程或其他适用于甲方的法律法规或判决等相冲突；

B、与甲方同第三人所签署的任何法律文件如保证协议、承诺、合同等中的义务相冲突或导致任何违约，或使乙方的权利受到约束。

5. 技术资料

5.1 本合同项下技术资料（除合同特殊条款规定外）将以下列方式交付：合同生效后 7 天之内，乙方应将提供服务所使用的软件或软件系统的中文技术资料一套，包括但不限于目录索引、图纸、操作手册、使用指南、维修指南、服务手册和示意图（若双方关于该等技术资料清单有明确要求的，以该要求为准，若未约定的，乙方所提供的技术资料应符合行业规定且保证甲方相关人员能依据该等技术资料使用）免费寄给甲方。乙方须在合同签订后 7 天内，制订出提交资料的进度表，此进度表应符合项目进度的需要并经甲方认可。

5.2 如果甲方确认乙方提供的技术资料不完整或在运输过程中丢失，乙方将在收到甲方通知后 7 天内将这些资料免费寄给甲方。

5.3 乙方提供的所有资料都需中文正本，若为外文需由甲方翻译成中文。

6. 保险

6.1 如乙方未按照本合同条款进行投保，因乙方未投保导致的一切后果与相关责任将均由乙方承担。

6.2 如果乙方交付的技术资料在运输途中发生丢失或损坏，乙方应与承运部门及保险公司联系进行索赔，甲方协助乙方收集相关证明，同时乙方应尽快向甲方补供以满足需要。如果此种丢失或损坏不属于保险公司的赔偿范围，则乙方应负责对甲方进行赔偿。

6.3 乙方须对其任何雇员或其他帮助、服务人员的意外或伤亡承担全部责任。甲方对乙方雇员的意外或伤亡，不论该人是否受聘于乙方，均不负有任何法律上的赔偿责任；乙方须保障甲方免负任何有关的索赔、主张、诉讼、费用和支出。

6.4 乙方均须为从事本合同相关工作的所有雇员购买及维持所需的保险。如有任何从事本合同相关工作的雇员或其他人士受到损伤，乙方应自行解决或通过有关合法途径取得此部分费用。

7. 培训

乙方应按照本项目招标文件技术部分关于培训的要求，以及投标文件中有关对培训的相应内容安排培训。具体的培训时间、内容及人员安排等应以甲方的书面通知为准。若乙方的培训效果不能满足双方约定或甲方实际掌握该等货物的使用等需要时，乙方承诺为使培训达到该等目标而开展多次且有效之培训。

培训安排在北京广播电视台内进行，且不再单独报价。

8 项目之相关变更

8.1 为了维护和兼顾各方的利益，确保应用系统集成服务的质量，在本合同签署后，甲、乙双方均有权在履行本合同的过程中合理地提出变更、扩展、替换或修改本项目的某些部分的请求，包括增加或减少服务的相应内容、提高或提升有关技术参数、变更交付或安装的时间与地点。

8.2

1) 若甲乙双方提出部分服务内容的变更建议，提出方应该将变更请求以书面形式提交给对方。

2) 其内容包括该变更对合同价格、项目交付日期、软件性能、系统集成的性能、项目技术参数的影响和变化以及对合同条款的影响等；

3) 接收方应当在 3 个工作日内对此做出书面回复；

4) 提出方在收到接收方的上述回复后，以书面方式通知接收方是否接受上述回复。如果接受上述回复，则双方应对此变更以书面形式确认，并按变更后的约定履行本合同。若导致合同价格变动，双方需签订补充协议，若不接受回复按原合同执行。

8.3 如果不属于合同范围内的合同技术要求或可推断需要研发的部分，项目变更报价需协商调整，双方需签补充协议。无论是哪一方提出上述变更的建议，凡涉及调整合同价款的，均应以本次投标的计价原则、计价标准为依据。

9 违约赔偿

9.1 如甲方不能按本合同规定如期如数得到合同规定的支持服务，视为乙方违约，乙方须向甲方支付违约金，违约金的计算办法为每延迟一天按合同额的 0.1%计算，不足一天按一天计算。超过 30 日的，甲方有权解除合同，并要求乙方支付合同总金额【20%】的违约金。

9.2 如发生违约事件，守约方要求违约方支付违约金时，应以书面方式通知违约方，内容包括违约事件、违约金、支付时间和方式等。违约方在收到上述通知后应于 3 天内答复对方，并支付违约金。如双方不能就此达成一致意见，将按照本合同所规定的争议解决条款解决双方的纠纷，但任何一方不得采取非法手段或以损害本项目的方式实现违约金。

9.3 如果在甲方发出索赔通知后 7 天内，乙方未做答复，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 30 天内或甲方同意的更长时间内，按照本合同规定的任何一种方法解决索赔事宜，乙方在此同意甲方将从合同款或从乙方开具的履约保证金保函中扣留索赔金，如果这些金额不足以支付索赔金额，甲方有权向乙方提出不足部分的追偿。

9.4 乙方违反本合同所规定的保密义务，应按本合同总价的 1%支付违约金。如实际损失超过该违约金的，甲方除可要求乙方支付上述违约金外，还可要求乙方赔偿因此所造成甲方的损失。

9.5 其他违约

乙方违反本合同项下除上述违约事项外的其他任何义务，情节较轻且未对甲方造成实际损害的，甲方给予书面提示告知；但超过三次或业已造成损失的，甲方除可要求乙方承担赔偿外，还可要求乙方承担不低于本合同价 5%的违约金，情节特别严重或造成甲方重大损失的，甲方除可要求乙方承担赔偿外，还可要求乙方承担不低于本合同价 20%的违约金，且可单方解除合同而不承担任何责任。

9.6 若乙方负责人员不配合甲方工作或不能胜任工作的，甲方有权要求乙方更换相关人员，乙方应在甲方要求更换之日起 5 日内更换。否则，甲方有权从未付的合同价款中扣除相当于 5000 元/每人次的违约金，若乙方此行为已造成甲方损失的，甲方还可另行向乙方索赔。

9.7 若乙方人员在甲方现场出现包括但不限于打架斗殴、毁坏、偷盗财物违反社会秩序，侵犯人身和财物安全的情况时，所产生的人员、财产损害由乙方自行承担责任并负责赔偿；由此造成的甲方或乙方的损失，由乙方负责全额赔偿，因此给甲方带来不良影响的，乙方应予消除。

9.8 乙方在此不可撤销地承诺：乙方应向甲方支付的违约金及赔偿金，甲方有权直接在任何应付未付乙方的款项中直接扣除，该等款项不足以支付上述违约金和赔偿金的，甲方可继续向乙方追偿。

10. 合同金额及支付方式

10.1 价格

本合同为固定总价合同，合同总价款为人民币 2389500 元整（大写：贰佰叁拾捌万玖仟伍佰元整）。

10.1.1 双方在此确认，本合同总价为固定总价，包含了乙方为完成本项目而可能支出的一切费用，包括但不限于税费、技术资料费的相关费用，以及服务过程中发生的人工费等所有交付前发生的费用。

10.1.2 双方在此确认，合同总价中已包含了乙方履行和完成本合同时所不能或

缺的所有附带工作的费用，不论该工作是否在本合同中有所说明，也不论是否在签订本合同时是否可以预料到。

10.1.3 本合同签订后国家任何政策性调整以及人工费价格涨跌均不能成为乙方调整本合同单价的原因。

10.2 支付方式：

详见合同特殊条款。

11. 履约保证金

11.1 乙方应在合同签订之日起 5 个工作日内，按约定的方式向甲方提交合同履约保证金，保证金金额详见合同特殊条款。

11.2 履约保证金用于补偿甲方因乙方不能履行其合同义务而蒙受的损失。如果乙方未能按合同规定履行其义务，甲方有权从履约保证金中取得补偿。

11.3 履约保证金应使用人民币，可选择下述方式提交：支票或电汇。

11.4 履约保证金在双方约定的服务质量保证期期满前应完全有效。如乙方违反前述约定，则乙方应在收到甲方书面通知之日起三日内向甲方以现金方式提交全部履约保证金。每迟延一天，乙方应向甲方支付本合同总价百分之一的违约金直至实际交付之日止。

11.5 履约保证金的退还：详见合同特殊条款。

12. 税费

与本合同有关的一切税费均适用中华人民共和国法律的相关规定。本合同项下所生一切税费均由乙方承担。

13. 保密条款

13.1 信息

13.1.1 乙方有权根据本合同的规定和项目需要，向甲方了解有关情况，调阅有关资料，向有关职能人员调查、了解甲方现有的相关据和资料，以对该系统

进行全面的研究和设计。甲方应予以积极配合，向乙方提供有关信息与资料，特别是有关甲方对系统深化的功能和目标需求方面的信息和资料，但如甲方对乙方完成本合同所需的甲方所有的信息和资料不予提供，则由甲方承担不予提供的损害后果。

13.1.2 在本合同的履行期内，任何一方可能获得与本项目相关的对方的重要秘密，对此双方皆应谨慎地且因为履行本合同目的之需要进行披露和接受。

13.2 保密

由甲方向乙方提供的图纸、详细资料和所有与本项目相关的、甲方的商业资料以及其他资料，被视为保密资料，仅被用于甲方或合同所规定的用途，除非得到甲方的书面同意，不能向任何第三方透露。否则甲方有权追究相关法律责任。

13.3 上述保密义务不适用以下情况

13.3.1 获取该信息一方在对方披露之前，已经通过正当、合法渠道知晓该信息；

13.3.2 获取该信息一方可以通过其他合法渠道获取该信息；

13.3.3 获取该信息一方从第三人处合法获取，并且不承担保密义务；

13.3.4 该信息所有人在对方获取该信息前已向第三人披露过的，且第三人不承担保密义务；

13.3.5 该信息为获取信息方独立开发或获取的信息；

13.3.6 法律强制披露；

13.3.7 经披露方书面许可。

13.4 信息安全

13.4.1 甲、乙双方同意采取相应的安全措施以遵守和履行上述条款所规定的义务。经一方的合理请求，该方可以检查对方所采取的安全措施是否

符合上述规定的义务。

13.4.2 任何一方可以根据其经营需要对外披露本合同的存在或其性质，但本合同的具体条款属于保密范围，未经对方的书面同意，不得向第三方披露。但以下情况除外：

13.4.2.1 法院或政府有关部门的要求；

13.4.2.2 法律规定；

13.4.2.3 一方向为自己服务的法律顾问披露，但应要求其承担保密义务；

13.4.2.4 一方向为自己服务的会计、银行、其他的金融机构及其顾问（采取保密措施）披露，但应要求其承担保密义务；

13.4.2.5 当事人实施收购、兼并或相类似的行为（采取保密措施）。

14. 知识产权

14.1乙方为履行此合同，向甲方提供服务所需使用的软件及相关技术未侵犯任何第三人的知识产权，甲方（包括最终使用方）依据本合同及双方约定的其他文件对该技术包括但不限于使用、收益、处分的行为，不存在任何侵权可能和被任何第三方追究任何法律责任。

14.2如任何第三方提出上述条项下的任何权利主张，则乙方须负责与第三方交涉处理此事，并承担一切由此引起的法律上和经济上的责任，从而使甲方免受由于第三方索赔从法律及经济责任上所遭受的任何损害。

14.3 若有第三方声称甲方使用乙方开发或提供的软件侵犯了第三方的知识产权或其它财产权利的，乙方不仅应直接参与纠纷的解决，还应承担由此产生的全部法律责任；如给甲方造成损失的，乙方应承担赔偿全部损失的责任。

14.4 甲方享有本项目开发实施过程中产生的全部知识成果的知识产权，包括但不限于著作权、专利权、专有技术等权利以及软件源代码和各种技术文档资料所有权。乙方非经甲方同意，不得以任何方式向第三方披露、转让

和许可有关的技术成果、计算机软件、秘密信息、技术资料和文件。

15. 合同的修改

甲方和乙方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，作为合同的补充，并报有关部门备案。

16. 合同的解除与终止

16.1 经甲乙双方协商一致，可以解除合同。

16.2 合同履行期内发生不可抗力且不可抗力事由持续 60 天以上致使合同无法继续履行，甲方可通知乙方解除合同。

16.3 出现本条款下列情形的，甲方有权以书面通知乙方的方式解除本合同：

16.3.1 因政府行为导致本项目终止、甲方无法继续参与本项目或本合同目的无法实现的；

16.3.2 乙方出现下列违法或违约情形时，甲方有权立即以书面通知乙方的方式解除本合同，同时保留向乙方追诉的权利：

16.3.2.1 违反中国法律、法规、规章有关禁止性规定的；

16.3.2.2 乙方拒绝按照甲方书面要求更换或移走不符合合同文件规定的货物而使本项目受到实质性影响的；

16.3.2.3 乙方未能在合同规定的限期或甲方同意延长的限期内，提供全部或部分服务，按合同规定可以解除合同的；

16.3.2.4 乙方未能履行合同规定的其他主要义务的；

16.3.2.5 在本合同履行过程中有腐败和欺诈行为的。

“腐败行为”和“欺诈行为”定义如下：

A、“腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签订、履行过程中的行为。

B、“欺诈行为”是指为了影响合同签订、履行过程，以谎报事实的方法，损害甲方的利益的行为。

16.4如甲方根据本合同相应条款享有解除本合同的权利，则在此种情形下甲方有权停付到期应向乙方支付的合同价款，并有权索回将在执行本合同过程中预付给乙方的合同价款。部分解除合同的，乙方应继续履行合同中未解除的部分。

16.5如果乙方破产导致合同无法履行时，甲方可以书面形式通知乙方终止合同而不给乙方补偿。该合同的终止将不损害或不影响甲方已经采取或将要采取的任何行动或补救措施的权利。

17. 不可抗力

17.1 由于地震、台风、水灾、火灾、战争以及其他由合同当事人不能预见并对其发生和后果不能预防、不能克服或不可避免的客观情况，直接影响本合同的履行或者不能按照合同的约定履行时，遇有上述不可抗力的一方可以免除相关合同责任。但遇有上述不可抗力的一方应于事故发生后七天内书面通知对方。并在 15 天之内提供不可抗力的详细情况及合同不能履行，或者部分不能履行，或者需要延期履行的理由和有效的证明文件。按不可抗力对履行合同影响的程度，由双方协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。一方在其延迟履行本合同后或迟延履行本合同时发生不可抗力的，迟延方的合同义务不能免除。

17.2 受到不可抗力影响的一方，应尽可能地采取合理的行为和适当的措施减轻不可抗力对本合同的履行所造成的影响。没有采取适当措施致使损失扩大的，该方不得就扩大损失的部分要求免责或赔偿。

18. 争议解决条款

如果合同双方在履行本合同过程中发生争议，双方应首先采取友好协商的方式解决该争议。如果上述争议在开始协商后 7 天内仍得不到解决，双方同意向北京市朝阳区人民法院提起诉讼。除争议事项或争议事项所涉及的条款外，

双方应继续履行本合同项下的其他义务。

19. 转让与分包

本合同不能转让和分包。

20. 计量单位

除技术规范中另有规定外,计量单位均使用国家法定计量单位。

21. 通知

21.1为享有本合同所规定的权利及履行本合同所规定的义务或有关违约交涉而需通知另一方时,通知方应采取书面形式,以中文书写,以特快专递(中国邮政 EMS)送达,且自发送之日起三个工作日即视为送达;以传真方式送达的,自传真机打印出文件发送成功记录时为送达。

21.2 双方在此一致确认,双方的联系地址、方式和联系情况详见合同特殊条款:

如一方欲改变上述信息的,应 3 日内以书面方式通知另一方,否则造成的后果自行承担。

22. 适用法律

本合同的订立、效力、解释、履行和争议的解决均适用中华人民共和国内地法律。

23. 廉洁自律

各方应自觉遵守法律法规、遵守新闻从业人员廉政行为若干规定及职业道德自律公约,互相监督,杜绝违反法律法规、违反上述规定及公约的行为。

24. 合同生效及其他

24.1 本合同内容的确定应以招标文件和投标文件为基础,不得违背其实质性内容。本合同经双方法定代表人或授权代表签署、加盖单位印章后生效。

24.2 本合同如有未尽事宜,经双方友好协商,另签订补充协议。补充协议与

本合同具有同等法律效力。

24.3 本合同壹式肆份，具有同等法律效力。甲方和乙方各执贰份。

第三部分 合同特殊条款

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

1.定义

本合同中的下列术语应解释为：

1) “甲方”系指：北京广播电视台。

2) “乙方”系指：奇安信网神信息技术（北京）股份有限公司。

3) “现场”系指：本合同项下的服务地点为北京市朝阳区建国路 98 号,北京广播电视台国贸办公区。

2.服务内容：

详见附件二《技术方案》。

3.服务时间：

服务期：自 2025 年 1 月 1 日起，至 2025 年 12 月 31 日止。在服务期内，乙方应按甲方要求提供 7×24 小时的技术服务。

4.服务地点：

北京市朝阳区建国路 98 号，北京广播电视台国贸办公区。

5. 合同金额及支付方式

5.1 合同金额：

本合同为固定总价合同，合同总价为人民币 2389500 元整（大写：贰佰叁拾捌万玖仟伍佰元整）。

5.2 结算方式：

1) 支付方式：合同生效之日起 15 日内，甲方向乙方支付合同总价的 50%

（￥1194750 元；大写：人民币壹佰壹拾玖万肆仟柒佰伍拾元整）；

2) 合同期满且甲方对乙方提供的服务及服务验收合格后 15 日内，甲方向乙方支付剩余 50%（￥1194750 元；大写：人民币壹佰壹拾玖万肆仟柒佰伍拾元整元整）。

3) 甲方付款前，乙方应提前出具同等金额的增值税专用发票，否则，甲方有权延迟付款且不承担任何责任。发票开具单位、开户行账号信息应与合同中相应信息一致。

6.验收：

服务期满后一个月内由乙方在项目实施地点组织召开项目验收会，参会人员由甲方代表及相关专家组成(专家费用由乙方支付)，相关人员对乙方提供验收材料进行现场审核，验收内容主要为网络安全服务履约情况，乙方提供的验收材料要能够客观、量化说明服务实施情况，验收会后由专家出具本项目的验收意见作为验收依据，经甲方确认后验收完毕。

本合同项下各项工作乙方需要交付验收材料，详见附件二《技术需求》。

7. 履约保证金

本项目不需履约保证金。

8. 争议解决

因本合同或在本合同履行过程中发生的任何争议，双方一致同意由甲方所在地有管辖权的人民法院管辖。除争议事项或争议事项所涉及的条款外，双方应继续履行本合同项下的其他义务。

9.通知与送达

双方的联系地址、方式如下，如一方联系方式发生变更，应及时通知另一方，如未及时通知，仍以以下联系方式为准：

甲方联系地址：北京市朝阳区建国路 98 号

甲方项目负责人：张益恺

甲方联系电话：13910026003

乙方联系地址：北京市西城区西直门外南路 26 号院 1 号楼 2 层

乙方项目负责人：刘腾飞

乙方联系电话：13681274341

第四部分 附件

附件一 分项费用明细

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	安全规划服务	23,500.00	1次/年	23,500.00	无
2	安全咨询服务	3,000.00	12次/年	36,000.00	无
3	安全运维技术服务	1,000,000.00	1年	1,000,000.00	无
4	渗透测试服务	1,500.00	50个系统/年	75,000.00	无
5	重要时期保障服务	15,000.00	6次/年	90,000.00	无
6	实战攻防演习支撑服务	50,000.00	4次/年	200,000.00	无
7	应急演练与应急响应服务	3,000.00	5次	15,000.00	无
8	红队评估服务	60,000.00	2次/年	120,000.00	无
9	迎检专项服务	150,000.00	1次/年	150,000.00	无
10	安全设备服务	80,000.00	1年	80,000.00	无
11	终端防病毒服务	200,000.00	1次	200,000.00	无
12	移动端安全加固服务	70,000.00	2个/年	140,000.00	无

13	信息系统等保测评	85,000.00	2个/年	170,000.00	无
14	容器安全检测服务	50,000.00	1年	50,000.00	无
15	蜜罐服务	40,000.00	1年	40,000.00	无
总价（元）				2,389,500.00	无

甲　方：北京广播电视台

名　称：（盖章）

法定代表人或

授权代表(签字)：

2025 年 1 月 26 日

乙　方：奇安信网神信息技术（北京）股份有限公司

名　称：（盖章）

法定代表人或

授权代表(签字)：

2025 年 1 月 23 日

附件二：技术方案

（一）安全规划服务

乙方需为甲方提供网络安全评估、规划和实施的全方位咨询服务，包括现状调研分析、安全架构设计、整体规划制定以及专项技术方案设计与实施支持。

技术要求：

乙方需结合国家网络安全相关政策、行业标准、行业案例等信息，在现场对北京广播电视台战略、业务、IP 运维和管理模式进行调研，完成北京广播电视台安全现状与差距分析。

乙方需结合当前行业前言技术、产品和业界最佳实践，根据广播电视行业的特点，从“技术、管理、运行”相结合的视角，进行安全架构的“概念设计、逻辑设计、实现设计”，制定网络安全规划方案，并明确总体安全提升方向、路线、年度重点安全建设任务，规划内容包括但不限于网络安全发展战略、管理制度体系、技术体系和运营体系，作为北京广播电视台安全建设的指导性文件，指导未来整体网络安全工作。

乙方需根据北京广播电视台的业务需求、环境、域划分原则、安全现状、面临的安全风险威胁、安全整体规划等内容，协助北京广播电视台在数据中心安全、云计算安全、数据安全等领域设计专用场景方案；设计方案需要符合国内相关法律法规、行业标准、北京广播电视台相关安全规划；提供方案实施过程中的技术支持与指导，协助客户解决实施过程中遇到的问题。同时，对实施后的效果进行评估，确保安全方案达到预期目标。根据评估结果，提供必要的调整建议，持续优化安全方案。设计方案至少包括安全目标、设计原则、具体方案、实施步骤、预期效果等内容。

服务频次：

服务期内提供不少于 1 次规划服务，3 次细分领域安全方案设计服务，全年提供现场服务工作量应不少于 60 人天。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台网络安全规划报告》

《北京广播电视台信息安全各阶段规划实施报告》

《安全设计方案》

（二）安全咨询服务

乙方需为甲方提供全面的网络安全咨询服务，包括架构安全、系统安全和安全事件处置等方面的专业分析和建议，以提升其整体网络安全防护能力并确保业务稳定运行。

技术要求：

乙方需具备广播电视行业网络安全需求的分析能力，能够理解并分析北京广播电视台的安全威胁、行业法规要求以及业务系统的特殊需求，依据北京广播电视台安全现状，提出设想及实现举措，以提升北京广播电视台网络安全防护能力，确保广播电视业务的稳定运行和数据安全。至少提供如下咨询能力：

（1）架构安全咨询能力

乙方需根据北京广播电视台现有的及规划中的 IT 架构，包括但不限于云环境、物理数据中心、制播网络等网络架构，从业务需求和风险分析，制定全面的架构安全策略，确保架构设计与业务目标相匹配，同时满足安全要求；针对现有架构的安全弱点，提出优化建议，如加强访问控制、优化网络拓扑等，以增强整体安全防御能力；确保架构设计符合相关法律法规及行业标准要求。

（2）系统安全咨询能力

乙方需从操作系统、数据库、应用软件、网络设备、中间件等各个系统层面，为系统安全策略的制定提供专业建议，确保策略的有效性和适应性，同时满足业务需求和安全要求；基于行业最佳实践，提供系统安全配置、管理、监控等方面的咨询，帮助北京广播电视台提升系统安全水平。

乙方需协助北京广播电视台制定和完善数据安全管理政策、流程和规范，

确保数据在收集、存储、处理、传输和销毁等各个环节均符合法律法规和行业标准要求；协助北京广播电视台建立供应链安全通报机制，确保供应链中的漏洞信息、补丁信息、病毒信息及时、准确地传达至北京广播电视台。

（3）安全事件咨询能力

乙方需针对上级单位下发的各类监管安全事件，服务期内针对此类安全事件，乙方需基于历史数据、事件内容，协助制定安全事件处置策略，识别事件根本原因、事件处理过程中的持续支持与指导、及时向上级单位报告事件进展及处置结果，同时，对事件处理过程进行复盘，总结经验教训，提升应对能力。

服务频次：

服务期内提供不少于 12 次咨询服务，全年提供现场服务工作量应不少于 48 人天。

交付物要求：

乙方需在服务完成后 20 天内提交《咨询报告》，如提供咨询服务期间未产生报告的，需交付《专家到场签到表》。

（三）安全运维技术服务

乙方需向甲方提供全面的安全运维技术服务，包括配备专业乙方安全团队（1 名项目经理和 4 名工程师）进行驻场服务，并开展安全巡检、漏洞扫描、基线核查等八大类具体服务工作，确保甲方网络安全。

技术要求：

（1）安全运维组织服务

乙方需提供 1 名专职项目经理对现场工作进行组织及计划制定，项目经理需提供不少于 250 人天（法定工作日八小时工作制）的驻场组织服务

交付物要求：

乙方需在服务期内半年及年终提交以下交付物：

《北京广播电视台安全服务工作总结（半年/年度）》

（2）基础运维服务

乙方需提供 4 名具备相应资质的运维服务工程师提供为期一年且不少于1000 人天（法定工作日八小时工作制）的驻场服务，服务时间需按照北京广播电视台要求开展。驻场服务人员工作时间须与北京广播电视台作息时间相同，未经北京广播电视台同意不能随意更换驻场工程师。

每月提供 1 次安全通告，通告内容包括操作系统、数据库系统、中间件、网络设备的漏洞信息、补丁信息、病毒信息等，使相关管理和技术人员及时了解最新的漏洞信息。

作为北京广播电视台网络安全服务的实施者，负责和业务厂商的日常工作协调工作；对需要通过等级保护测评的信息系统，在测评期间提供测评辅助服务。对安全服务工作进行每月、半年、年终做好相关总结工作。

交付物要求：

乙方需在服务期内每月、半年和年终提交以下交付物：

《北京广播电视台网络安全通告》

《北京广播电视台安全设备运维记录》

（5）互联网暴露面发现服务

乙方须通过现场方式，对北京广播电视台的外部环境进行评估和分析，以确定潜在的攻击路径和风险，通过对信息资产排查、疑似资产测绘等，对包含北京广播电视台相关信息的网盘、公众号以及外部开源社区进行监测，同时结合暗网数据，收敛外部暴露面，清查电视台相关服务，避免电视台相关数据泄露导致安全问题发生，服务期内提供不少于 1 次互联网暴露面发现服务。

交付物要求：

乙方需在服务完成后 20 天内提交《互联网资产暴露面报告》。

（6）漏洞扫描服务

乙方应根据北京广播电视台网络安全现状与操作系统现状，利用安全扫描工具，在保障漏洞库更新到最新的情况下对北京广播电视台所需检查的系统开展安全工作，扫描过程中不得影响业务系统正常运行，同时针对发现的安全漏洞开展安全漏洞的验证分析工作，根据不同安全风险出具解决建议，监督其他相关运维厂商进行整改，服务期内提供不少于 1500 台资产的漏洞扫描服务。

运维服务工程师利用安全扫描自动化工具对北京广播电视台全网业务系统应用程序、系统网络运行环境及虚拟化平台进行安全扫描服务，扫描业务系统存在弱口令、应用程序低版本、SQL 注入、跨站脚本、命令执行等安全漏洞和缺陷，将安全扫描结果以安全风险评估报告的形式提交北京广播电视台，并跟踪安全漏洞整改工作的完成情况。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台信息系统漏洞扫描实施方案》

《北京广播电视台信息系统季度漏洞扫描总结报告》

（4）安全巡检服务

服务期内由乙方安全团队每月对北京广播电视台资产运行情况进行安全检查，包括：定期对业务主机、网络设备和数据库系统等进行安全策略执行情况、资源使用等进行检查，对各系统配置策略等进行分析，发现安全问题时及时与北京广播电视台相关人员沟通并处理。

巡检检查的重点是安全设备的 CPU、内存状态、开放服务进行检查，对日志进行记录审计与归档，查看网站系统的运行情况，备份和维护安全设备配置，并做好版本管理，形成工作日志、维护记录单，服务期内每天对现有的 30 台安全设备进行巡检。

交付物要求：

乙方需在服务期中每天提交以下交付物：

《北京广播电视台信息系统安全巡检报告》

（5）安全加固指导服务

乙方需结合北京广播电视台渗透测试、安全巡检以及漏洞扫描等服务的检测结果和结论，根据安全基线要求，协助北京广播电视台相关部门及时消除系统中所存在的安全威胁，降低恶意攻击者利用安全漏洞威胁系统安全运行的几率，从而有效控制因各种潜在安全威胁引发的业务中断及信息外泄等风险，将高风险漏洞和中风险漏洞降低至可接受的范围内，使得整个网络、应用系统的安全状况提

升到一个较高的水平。安全加固须涉及对系统整体或所属资产进行加固，应至少包含网络结构优化调整、系统设备脆弱性加固、加固效果跟踪评价等内容。服务期内至少开展 300 台资产的安全加固指导服务。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台信息系统安全加固整改建议》

《北京广播电视台信息系统安全加固情况总结》

（6）基线核查服务

北京广播电视台资产数量较大，承载信息系统数量较多，为了统一标准，加强管理，乙方需要对业务进行充分调研的情况下，结合公安部、工信部等官方标准，针对服务器操作系统、数据库、应用中间件、网络设备、安全设备进行相关的安全基线检查，检查内容至少包括：OS 安全、帐号和口令管理、认证和授权策略、网络与服务、访问控制策略、通讯协议与路由协议、日志审核策略、加密管理、设备其他安全配置等。

乙方应根据安全基线核查结果提出具体的整改建议和方案，并协助北京广播电视台制定新的安全基线，作为新设备部署、上线的基本配置要求和安全加固标准。

乙方在技术方案中应明确检查范围、检查内容、检查手段等内容。

交付物要求：

乙方需在服务期内服务期内至少完成不少于 5 个安全基线的制定服务，并在服务期结束前提交以下交付物：

《北京广播电视台操作系统安全基线》

《北京广播电视台应用系统安全开发基线》

《北京广播电视台网络设备安全基线》

《北京广播电视台安全设备安全基线》

《北京广播电视台应用中间件安全基线》

《北京广播电视台数据库管理系统安全基线》

《北京广播电视台移动端应用安全基线》

（7）威胁事件监测服务

乙方在日常监测期间（除重要时期、攻防演习时期外的其他时间），应指定一名基础运维服务工程师提供此项服务，服务内容包括：应能通过对网络流量或告警日志进行实时动态分析，结合威胁情报、失陷主机行为特征分析规则和深度学习模型，发现隐藏在海量流量中的可疑活动和安全威胁，并对检测结果提供丰富的上下文信息与可视化分析，并进行持续监控，提升北京广播电视台对网络的检测与响应能力。

全年提供现场服务工作量应不少于 250 人天。

交付物要求：

乙方需在服务期中每天提交以下交付物：

《全流量安全威胁检测日报》

（8）策略梳理优化服务

乙方需对北京广播电视台开展全面而细致的网络现状调研工作。这包括但不限于对台内所有网络资产的彻底审查，详细了解其配置、性能和运行状态。同时，需深入分析业务流转的各个环节，确保对数据流向、业务依赖关系以及关键业务流程有一个全面的掌握。

乙方需在调研结束后绘制出详尽的网络拓扑图，清晰展示网络中的各个节点、连接方式以及数据传输路径。此外，对于网络中的关键安全组件，如路由策略、交换机的访问控制列表（ACL）策略，以及防护墙的配置策略，乙方都应进行深入的梳理和分析，确保每一策略都得到充分的理解和记录。

乙方需提交一份详尽的调研报告，其中应包含对现有网络环境的全面分析、安全策略的优化建议，确保北京广播电视台的网络安全工作能够有序、高效地推进，服务期内至少开展不少于 4 次策略梳理优化服务。

交付物要求：

乙方需在服务期结束前提交以下交付物：

《北京广播电视台基础网络安全策略梳理报告》

（四）渗透测试服务

乙方需在甲方授权下对 50 个系统（40 个办公域和 10 个公有云系统）进行全面的渗透测试服务，包括应用、中间件、主机和业务逻辑四大维度的安全检测。

技术要求：

乙方应在北京广播电视台授权的前提下有组织有计划对指定的业务系统进行渗透测试。确保在业务系统稳定运行的基础上从主机、应用、中间件、业务逻辑处理等维度开展非破坏性的安全检测，检查是否存在漏洞，并在测试完成后 3 天内提升渗透测试报告协助系统运维单位开展安全漏洞的整改加固工作与漏洞复测工作。

渗透测试内容包含但不仅限于如下场景：

应用渗透测试：包括 SQL 注入、XSS、XXE、CSRF、RFI、上传漏洞、信息泄露、远程命令执行、反序列化漏洞等。

中间件渗透测试：对 IIS、apache 等常见中间件进行已知安全漏洞验证和默认策略安全检测。

主机渗透测试：包括域传送漏洞、弱口令漏洞、未授权访问漏洞、脚本密码检查、本地提权漏洞、应用防护软硬件缺陷等。

业务逻辑安全：业务逻辑安全测试范围包括用户或口令枚举、弱口令测试、平行/垂直越权、未授权访问、验证缺陷、业务逻辑限制缺陷等。

服务频次：

服务期内提供不少于 40 个办公域业务系统、10 个公有云业务系统的渗透测试，需要包含初测及复测的全部工作。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《渗透测试初测报告》

《渗透测试复测报告》

（五）重要时期保障服务

针对各重要保障时期，乙方需向甲方提供全年不少于 50 天的 7*24 小时网络安全保障服务，组成重要时期保障服务团队执行安全监测、攻击分析及应急响应等工作。

技术要求：

根据公安部门、北京市政府等监管单位网络安全工作要求，结合北京广播电视台实际情况，开展如“两会”、“春节”、“国庆”、“服贸会”、“‘一带一路’国际合作高峰论坛”等重点安全保障期的重点网络安全保障工作，提供网络安全技术支持和现场人员值守保障，完成重保期全天的安全监测、攻击行为分析、静态特征分析、特为模式分析、事件处置等相应工作。服务内容要求：

1) 安全监测：通过现场值守模式在重要时期网络安全保障工作中，根据准确的研判分析能力，对攻击者的身份类型进行精准定位。
2) 攻击行为分析：通过本地流量切片分析+云端黑客档案情报+研判分析引擎分析+专业分析师分析，实现攻击者脸谱分析研判操作，输出攻击者脸谱信息。
3) 静态特征分析：提取攻击者留下的静态特征痕迹，如：C2 域名、Mac 地址、邮箱、手机号、Cookie、恶意文件 MD5、后门地址、XSS 平台地址、DNSLOG 地址等等。
4) 事件处置：利用现有检测措施在保障期间检测到异常的行为，开展协同分析和确认，并按照网络安全事件处置流程进行处置。
5) 应急响应：在重要时期乙方需提供对事件的不限次应急响应服务，当发现攻击者入侵到系统时，乙方需能够组织专业人员进行及时的现场应急响应，评估损失情况，降低安全事件影响，防止更多系统被入侵，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判，协助开展风险分析与业务整

改。

6） 重要时期保障服务为7*24小时不间断的现场值守服务。

7） 重要时期保障服务团队需由六名工程师组成，包括已有的四名驻场运维服务工程师及新增2名重保高级分析专家，按照“三班倒”的工作模式，每班不少于2人，开展现场值守工作。

服务频次：

服务期内提供不少于6次重要时期保障服务，现场服务工作量总天数不少于50天。

交付物要求：

乙方需在服务完成后20天内提交以下交付物：

《北京广播电视台重要时期安全保障方案》

《北京广播电视台重要时期安全值守工作总结》

（六）实战攻防演习支撑服务

针对监管机构组织的安全演习，乙方需向甲方提供全年不少于60天的7*24小时攻防演习支撑服务，组成实战攻防演习支撑服务团队进行三班倒值守，负责防护方案制定、现场防守、攻击分析、人员培训等工作。

技术要求：

根据国家广播电视总局、公安部门和其他监管机构不定期组织的网络安全演习工作要求，乙方需提供实战攻防演习支撑服务团队，全面协助北京广播电视台开展重保前培训、现场重保值守、安全监测、事件分析、攻击溯源、应急响应等，并协助北京广播电视台开展风险清理、体系优化及总结报告等，同时在服务过程中应指导北京广播电视台技术人员开展安全分析、攻击溯源等工作，进行知识技能转移。服务要求如下：

1） 根据北京广播电视台的网络架构、业务特点、安全需求及监管要求，设计全面、细致、可操作的防护方案。

2） 协助北京广播电视台开展现场防守工作，实时分析攻击态势，检测、监测

和分析攻击事件，协助北京广播电视台进行现场调度、应急处置等工作，并针对安全分析、调查取证、攻击溯源等技术对北京广播电视台开展不少于 1 天的人员技术培训，进行知识和技能转移

3) 协助北京广播电视台开展实时攻击态势监测，并协助北京广播电视台进行指挥决策；

4) 乙方应汇总并实时输出攻击监测和分析报告，通报发现的攻击行为，给出处置建议，并协助北京广播电视台开展攻击事件应急响应和处置，及时消除不良影响；

5) 应根据北京广播电视台要求采用混合分组等方式，指导北京广播电视台技术人员开展安全分析、调查取证、攻击追踪溯源、零日漏洞发现、非法攻击画像、技战法总结等工作，进行知识技能转移；

6) 利用流量、日志、报告等资源，协助北京广播电视台进行攻击现场清理，发现并消除安全隐患，总结整体重保工作情况，并根据重保中发现问题，协助北京广播电视台制定有针对性、可落地的安全体系改进建设指导方案。

7) 实战攻防演习支撑服务为 7*24 小时不间断的现场值守服务。

8) 实战攻防演习支撑服务团队需由六名工程师组成，包括已有的四名驻场运维服务工程师及新增 2 名攻防高级分析专家，按照“三班倒”的工作模式，每班不少于 2 人，开展现场值守工作。

乙方作为护网演习的主责方在北京广播电视台授权下开展护网防守工作，根据护网防守效果作为评价整体安全服务的重要指标项，北京广播电视台有权根据实际防守效果对乙方提供服务进行评价打分，护网期间如果出现重要系统被攻破，北京广播电视台有权在整体服务项目中扣除相应费用。

服务频次：

服务期内需提供不少于4次护网演习技术服务，现场服务工作量总天数不少于60天。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台网络安全演习防守方案》

《北京广播电视台网络安全演习安全事件分析研判报告》

《北京广播电视台网络安全演习总结报告》

（七）应急演练与应急响应服务

乙方需为甲方提供应急演练组织(每年至少1次)和应急响应服务(每年5次)，包括演练环境搭建、应急预案制定与评估，以及7×24小时的应急响应处置。

技术要求：

（1）应急演练

乙方应在北京广播电视台指定的场景下搭建应急演练环境，模拟发现确切的安全事件的情形，组织开展安全应急演练工作，检验北京广播电视台安全保障体系是否具备安全事件的监测能力、应急演练预案是否合适、安全运维人员是否有基本的安全事件处置能力等。应急演练内容应不限于应急演练方案的制定、演练用例的生成、演练结果的评估等。并在演练结束后，应提供安全应急演练过程、安全保障体系缺陷、应急预案弱点、安全运维人员的安全事件处置能力评测以及相应的改进建议的应急演练报告。

（2）应急响应

乙方应具备 7×24 小时的应急响应协同处置能力水平。当北京广播电视台发生大规模病毒爆发、网站被篡改、数据被恶意删除等确切的安全事件时，乙方应能够快速安排应急响应人员及时采取行动，限制事件扩散和影响的范围，控制潜在的损失与破坏，并协助开展安全事件攻击行为的溯源分析工作。乙方应在接到北京广播电视台应急响应电话通知后 10 分钟做出响应，1 小时内到达现场开展响应处置工作。主要服务内容包括：

1) 提供现场排查分析、制定响应策略等工作，通过对现场安全事件情况进行排查分析，确定安全事件类型，评估安全事件可能产生的影响，并针对事件制定详细的应急响应策略。
2) 提供抑制方案的制定与实施等工作，现场应急专家及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，并确保封锁方法对涉及相关业务

影响最小。

3) 提供根除方案制定、实施以及效果判定等工作，根据事件抑制情况以及有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

4) 协助客户选择合适的系统恢复方案对客户系统进行恢复。

5) 提供应急响应事件报告输出工作，现场应急专家通过对以上各阶段处理过程进行记录总结，并整理与事件相关信息及时反馈给客户。

服务频次：

服务期内提供不少于 1 次应急演练组织服务，5 次应急响应服务。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台应急演练方案》

《北京广播电视台应急演练总结》

《北京广播电视台应急响应报告》

（八）红队评估服务

乙方需为甲方提供每年至少2次的红队评估服务(其中1次需由第三方完成)，通过模拟APT攻击等方式对系统进行安全评估，全年总工作量不少于80人天。

技术要求：

乙方需描述北京广播电视台的网络技术架构和业务现状，根据面临的主要网络安全威胁和护网演习要求制定有针对性的红队评估服务方案，上述要求需在技术方案中明确体现。

乙方使用入侵者的攻击方法对北京广播电视台业务系统及网络运行环境进行风险可控的入侵。乙方应提供经验丰富的渗透工程师，通过互联网，利用台方授权许可的各种黑客手段，以及人工的经验对指定的目标进行红队评估，最终发现可以被利用的各种安全风险和安全隐患。攻防演练完成后将入侵的详细过程和细节以报告的形式提交给北京广播电视台。

组织经验丰富的网络攻击专家技术团队，经过台方授权并签订保密协议的

前提下，指定关键业务作为标靶开展模拟攻击测试。不告知我台网络相关信息的情况，通过获取暴露在公网上的信息，运用网络攻击技术对北京广播电视台所属网络系统进行端口扫描、口令暴破、渗透攻击和社会工程等技术进行攻击。

通过实战化方式，最大限度模拟APT攻击手法，以专业的团队视角对北京市广播电视台网络安全防护情况进行监测。以不采用破坏性攻击为底线，利用系统提权、控制业务、获取数据为目标的攻击手段，最大程度暴露安全风险及安全防护短板，深入评估安全防护能力。

服务频次：

服务期内提供不少于两次红队评估技术服务，全年服务工作量不少于80人天。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台红队评估服务报告》

《北京广播电视台红队评估问题汇总》

《北京广播电视台红队评估加固建议》

（九）迎检专项服务

乙方需为甲方提供每年至少 1 次的迎检专项服务，从六个主要纬度((终端、流量、外联、邮件、策略、供应链）提供迎检服务，并输出专项服务报告。

技术要求：

乙方需派遣专业技术人员通过安全自查工具、文档查验、人员访谈、现场核查等方式进行关键信息安全检查，防止关键信息泄露、失窃事件的发生。检查内容包括：终端安全、流量安全、违规外联、邮件安全、策略梳理、供应链安全，服务期内提供不少于 1 次迎检服务。具体要求如下：

（1）终端安全

乙方需针对目标终端进行深度数据采集和分析，识别所选取的终端安全威胁

状态；将终端区分为“存在恶意文件”、“存在恶意行为”和“无风险”三种状态；并协助北京广播电视台进行专项清理（至少包括工具查杀及人为处置）。测试的终端不少于 1000 个。

服务工具要求：

1) 所提供的终端工具 Agent 安装包不超过 20M，日常运行时 CPU 占用≤1%，内存占用≤200MB，仅运行 EDR 模块 CPU 占用≤0.5%，内存占用≤30MB。全部满足得分，否则不得分；
2) Agent 支持静默安装包，也支持随时开启和关闭静默运行模式，并要求具备核心进程的隐藏功能。
3) 要求工具上支持自定义响应动作，并可指派给对应的终端或者终端分组进行安全事件的快速响应。响应动作包括但不限于：隔离终端、阻断网络连接、隔离文件、隔离进程、禁用服务、清理注册表项/值等，并支持对以上所有动作进行逆向操作。
4) 要求终端可采集操作系统的基础行为日志，包括：进程创建、进程退出、驱动加载、映像加载、文件创建、文件删除、注册表项创建、注册表项删除、注册表值删除、注册表值修改、注册表项重命名、磁盘读取、文件创建时间修改、网络访问、文件流创建、账户登录。要求提供产品对应能力的截图

（2）流量安全

乙方需针对目标系统的网络流量进行监控，识别 DDoS 攻击、恶意软件传播、数据泄露等网络安全威胁，同时提供流量行为分析报告，协助网络性能与安全性。

（3）违规外联

乙方需针对目标系统进行监测，识别内网外联互联网行为，告警并生成详细分析报告。

（4）邮件安全

乙方需配合北京广播电视台完成对邮件系统的安全检测，包括但不限于邮件内容的实时监控、病毒和恶意软件的检测与防御、数据泄露防护等。

（5）策略梳理

乙方需以等保、分保测评要求为基准，对现有安全产品的配置、安全策略进行调整优化至最佳，达到安全可用的符合相关要求的实战化运行目标。服务完成、输出策略评估整改报告。

（6）供应链安全

乙方需将采集到的终端数据与多源威胁情报进行碰撞、交叉验证，识别终端主机威胁数量和威胁类型，包括 APT、黑灰产软件、传统僵木蠕、PUA 软件、流氓软件、勒索挖矿等恶意程序等。并协助北京广播电视台进行专项清理（至少包括工具查杀及人为处置）。

服务频次：

服务期内提供不少于一次迎检专项服务。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《北京广播电视台迎检专项服务报告》

（十）安全设备服务

乙方需在服务期内部署安全设备提供安全服务，包括态势感知分析服务(不少于 2 台态势感知平台、4 台流量采集探针)和边界防护服务(不少于 1 台防火墙、1 台上网行为管理设备)，通过这些设备实现全面的安全检测、监控和防护。

技术要求：

乙方需在服务期内以部署安全设备方式提供安全设备服务。乙方需根据北京广播电视台现有业务所面临的安全风险，明确提出所需要的设备和技术措施，结合本次所提供的设备服务，制定出切实可行的部署方案，并明确相应安全防护效果，上述要求需在技术方案中明确体现。

（1）态势感知分析服务

乙方需在服务期内提供安全态势感知平台设备满足安全事件检测、预警、响

应需求，所提供安全态势感知分析平台设备不少于 2 台，全流量采集探针硬件设备数量不少于 4 台，提供不少于 35 个端口镜像端口的采集能力，流量解密设备 2 台，满足主要区域间的流量监测需求。上述设备均需要为硬件，且在北京广播电视台现场部署。

服务要求：实现复杂多元异构数据的采集，如检测信息、告警信息、审计信息，利用分析引擎，结合威胁情报，实现对北京广播电视台全域的高级威胁深度检测；通过资产风险管理的持续监控，可实现安全事件发生时的精确实时定位；实现全局安全风险态势感知，并将安全态势以可视化方式展现；乙方需协助北京广播电视台建立事件处置流程，结合协同处置机制，实现对安全事件的快速处置。

1. 态势感知分析平台设备

序号	安全态势感知分析平台技术规格要求
1	乙方所投设备为自有设备，存储容量不小于 48T。 标准 2U 机架式设备，CPU 不少于 1 颗，不少于 16 核。内存不小于 96GB，系统盘不小于 960GB SATA SSD，数据盘不少于 6*8TB，标配盘位数不少于 12，冗余电源，接口不少于 4 千兆电口，最大日志处理速度≥ 18000EPS。
2	支持对重保任务的增删改操作，任务分战前、战中、战后三个阶段，支持对任务记录的导出查看及多个任务并行等功能
3	# 支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为。（需提供功能截图证明并加盖乙方公章）
4	支持以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产。
5	# 支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击带外分析。（需提供功能截图证明并加盖乙方公章）
6	支持挖矿行为的分析，分析内容包括挖矿阶段、币种分布、挖矿告警趋势以及挖矿告警信息。
7	支持对告警进行加白。
8	支持远程工具分析。
9	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。
10	支持对 http、pop3、smtp、Telnet、ftp、imap 等协议弱口令分析，且能够自定义弱口令字典。
11	支持资产横向访问分析，能展示源资产 ip、目的资产 ip、端口、协议、banner、时间等详细信息，且能自定义源 ip 白名单。
12	支持可疑来源访问行为分析，能展示来源、源 IP、资产 IP、资产组、源地域、目的端口、URI 等信息，且能自定义可疑来源。
13	# 支持对任意线索的自定义拓线及溯源取证分析，支持以可视化分析画布形式展示拓线过程并支持结果快照导出；支持对于给定线索的溯源结果展示，包括但不限于攻击溯源、失陷主机分析、暴力破解分析、弱口令分析等。（需提供功能截图证明并加盖乙方公章）
14	支持策略定义，可根据工作流进行处置动作定义，且能根据告警类型、攻击结果、威胁类别进行联动策略定义。
15	支持大屏展示网络攻击态势，包括整体网络风险指数、告警总数、攻击次数、攻击 IP 数、攻击源国家/地区 TOP5、攻击态势，并支持自动翻转的攻击全景地图展示。
16	支持展示自动发现、终端管理系统获取和人工录入的资产信息。
17	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。
18	支持与防火墙进行联动，发现威胁事件后支持对攻击 IP、恶意域名和受害资产的流量进行阻断。
19	基于深度学习的自然语言处理技术，提供文本对话交互功能，为用户提供告警威胁类的问答服务。

2. 全流量采集设备

序号	技术规格要求
1	乙方所投设备为自有设备，同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流（模拟企业级网络真实场景流量）吞吐量≥4Gbps；配置至少 6 个千兆电口，4 个万兆光口。
2	支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs、ICMP、SSL、SSH 等
3	支持对流量中出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件、文档类型文件、多媒体文件、脚本文件等类型。

4	支持通过 ip、ip 段、端口等进行流量过滤，过滤语法支持 and、or、not 等多条件过滤语句。
5	# 支持离线流量采集，可通过手动 PCAP 导入方式对离线流量进行采集（需提供功能截图证明并加盖乙方公章）。
6	支持自定义协议和端口，满足特殊场景下的流量抓取。
7	# 支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC，情报总量 370+万条（需提供功能截图证明并加盖乙方公章）。
8	支持检测针对 WEB 应用的攻击，如 SQL 注入、XSS、系统配置等注入型攻击。
9	支持基于工具特征的 WEBSHELL 检测，能通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等
10	支持基于 webshell 函数的攻击检测，如文件包含漏洞、任意文件写入、任意目录读取、任意文件包含、preg_replace 代码执行等
11	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
12	支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。
13	支持自定义漏洞规则。
14	# 支持门罗币、莱特币、以太坊、比特币、斯特币等二十余种币种的检测，区分挖矿行为阶段：恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额（需提供功能截图证明并加盖乙方公章）。
15	支持对 HTTP、FTP_DATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS 等类型协议的流量进行文件还原。
16	支持基于 IP 地址的旁路阻断，能够在实时镜像的流量中发现恶意 IP 并实现实时阻断。
17	支持自定义弱口令字典，支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测
18	支持攻击特征高亮展示，方便分析人员事件分析

3. 流量解密设备

序号	技术规格要求

1	乙方所投设备为自有设备，硬件要求：准 2U 机箱，冗余电源，标准配置≥2 个接口板卡扩展插槽，标准配置≥8 个 10/100/1000M 自适应电口，≥8 个千兆光口，6 个万兆光口；标准配置≥1 个 Console 口。
2	性能要求：网络层吞吐量≥70G，并发连接≥1900 万，每秒新建连接数≥55 万，SSL 解密吞吐量≥3G，SSL 会话数≥10 万；
3	支持路由、旁路、交换以及混合模式接入，满足复杂应用环境的接入需求。
4	支持冗余策略分析、命中时间分析、安全策略推荐，方便管理员针对当前中策略进行优化。
5	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。
6	支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，类型可选择 SSL 代理、SSL 入站检查、SSL 卸载和 SSL 加密，同时支持将解密后流量镜像到其他设备进行分析统计。
7	支持 SSL 解密策略，支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行 SSL 卸载，支持配置基于源安全域、目的安全域、源地址、目的地址、SNI 对象、服务、证书自学习。
8	支持算法类型是国际算法或国密算法，支持导入服务器证书或加密证书和签名证书，支持双向认证。
9	支持服务器证书功能，支持导入或删除证书，支持以上传文件、批量上传文件或从本地 CA 中心方式导入证书。
10	支持设置镜像端口偏移量，端口偏移范围在 0-60000 之间。
11	支持 HTTP 改写策略和 HTTP 改写规则，HTTP 改写规则支持设置改写频次、匹配操作符、匹配条件、改写动作、改写方式、改写内容。
12	支持 SSL 协商诊断，支持设置超时时间范围、异常包留存、NSS KEY 缓存。
13	支持设置检测解密对象，包括配置选项中针对不可信证书、不支持的版本、不支持的算法、证书有效期检查的允许或阻断，版本信息支持 TLS1.0/1.1/1.2/1.3 和 SSL3.0 的设置，支持算法预定义或自定义，支持和客户端或和服务端的会话复用。
14	支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。
15	支持配置基于 IP、用户、应用的流量管理规则，且至少支持对 2900 种应用定制流量管理规则。

（2）边界安全防护服务

乙方应提供一套边界防护设备，包括防火墙 1 台、上网行为管理设备 1 台，满足北京广播电视台基础防护的要求，需要通过漏洞防护、防间谍软件、反病毒、URL 过滤功能，基于本地安全引擎，能高效拦截常见漏洞入侵、间谍软件、病毒、木马、钓鱼网站、恶意 URL 访问等网络威胁。设备在北京广播电视台现场部署，在服务中应包含设备厂家的设备升级、现场巡检以及远程技术支持。具体要求如下：

1. 防火墙设备

序号	技术规格要求
1	乙方所投设备为自有设备，网络层吞吐量≥20G，并发连接≥700 万，每秒新建连接数 25 万，至少 8 个千兆电口，8 个千兆光口，6 个万兆光口
2	支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定
3	支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持 RIP v1/v2/ng，OSPFv2/v3，BGP4/4+协议；
4	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查
5	支持基于 IPv4/v6 地址、应用的会话限制，限制动作包每 IP 新建、每 IP 并发、所有 IP 新建、所有 IP 并发，且可以基于安全域指定限制方向
6	# 能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，以及对至少 6 级压缩文件进行解压查杀。（需提供功能截图证明并加盖乙方公章）
7	支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作，可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护

8	# 支持间谍软件防护功能，同时将间谍软件特征库分类，至少包括木马后门、病毒蠕虫、僵尸网络等三种分类;支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的间谍软件防护。（需提供功能截图证明并加盖乙方公章）
9	产品支持对常见 Web 应用攻击防御，支持漏洞防护功能，漏洞防护特征库及间谍软件库包含高危漏洞攻击特征。
10	支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息；
11	# 所投产品支持将其他硬件安全设备（包括但不限于防火墙、IPS、IDS、WAF、行为管理、流量探针等）加入网元组，并接受流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池（如 WAF 安全资源池），并将流量通过负载均衡（“源地址哈希”、“源目的地址哈希”，“加权源地址哈希”、“加权源目的地址哈希”、“加权地址端口哈希”、“轮询”和“权重轮询”）的方法编排给组内所有网元，（需提供该功能的第三方测试报告，加盖乙方公章）
12	# 所投产品支持灵活的服务链编排功能（服务量管理），支持串接链和旁路链，支持网元组的方向和目的位置设置。（需提该功能的第三方测试报告，加盖乙方公章）
13	# 所投产品支持灵活的细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、流量方向（内网到外网/外网到内网）的引流策略，并详细记录日志。（需提该功能的第三方测试报告，加盖乙方公章）
14	支持用户自定义重点 URL 分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL 分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。
15	支持接收针对突发重大安全事件的“应急响应消息”，针对该消息可以选择“自动”或“手动”处理。至少在界面显示安全事件的名称、类型、当前防护状态、处置状态以及相应的操作等信息；并自动检测、呈现针对该事件的处置结果，提示导致处置未生效的错误配置
16	支持作为轻量级“探针”与本方案中配置的态势感知平台联动，上报网络活动产生的数据至态势感知平台；并支持接收来自态势感知平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。

2. 上网行为管理设备

序号	技术规格要求
1	应用带宽≥1G，最大并发连接数≥60 万，新建连接数≥4 万，整机吞吐量≥15G，千兆电口≥6 个，内存≥8G，存储容量≥1T，数量不少于

	2 台。
2	设备需提供物理硬件 bypass 按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。需提供设备照片加盖厂商公章。
3	设备必须采用一体化引擎，避免在复杂应用场景开启多功能时的延迟损耗及性能衰减。
4	设备需支持以下部署模式：网关模式、镜像模式、网桥模式、多路桥接、Portal 模式等。
5	# 可集中呈现上网行为风险等级和状态； 行为风险等级包括安全等级、效率等级、合规等级和管控等级； 行为状态包括管控效果、运行状态、安全状态、泄密风险状态、合规状态和应用使用状态；可展示特征库规模详情。 （需提供功能界面截图加盖乙方公章）
6	需支持基于云端大数据安全平台，对恶意 URL 访问进行封堵和记录日志。
7	# 需支持接收来自态势感知平台的封堵指令。（需提供功能截图证明并加盖乙方公章）
8	需支持外发解密流量，为不具备解密条件的设备提供内容解析
9	应用协议库包含的应用数量不低于 12000 种，应用规则总数不低于 73000 种。
10	设备内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽 6 大类。
11	# 需支持基于大小的内容外发控制。不开启 SSL，对终端影响小；仅对外发控制，不影响浏览和下载等行为；（需提供功能截图证明并加盖乙方公章）
12	需支持基于文件后缀的文件类型识别；支持基于文件内容对归档文件、压缩文件、加密文件、脚本文件等 170+文件类型识别。修改后缀名，压缩等方式均可以识别准确类型。
13	# 需支持业务系统访问及 API 接口进行双向扫描、通过敏感信息、安全漏洞、行为接口、自定义接口规则等识别并标识数据及传输风险，（需提供功能截图证明并加盖乙方公章）
14	≥2.8 亿条 URL 数据，根据 URL 库及 URL 关键字进行网址访问管理，一条策略实现阻断、记录、告警，方便维护。
15	能够基于发件人、收件人、主题、内容、附件名维度进行过滤、记录、

	告警；能够支持 SSL 加密的 SMTP 邮件审计；
16	支持对 XShell 和 SecureCRT 客户端外发文件的动作和内容审计；
17	需支持 Https、ftp、telnet、DNS、SNMP、NFS、NETBIOS 的协议审计。
18	可生成网页访问、论坛发帖，webmail、邮件收发、应用访问、应用流量、通道分析等各种统计报表。
19	支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端；

（十一）终端防病毒服务

乙方应支持对北京广播电视台现有的防病毒系统的版本升级、防病毒特征库升级服务，向甲方全年提供不少于 508 台终端的病毒运维服务。

技术要求：

具体如下：

序号	技术规格要求
1	需提供与现有终端防病毒软件兼容的最新版本升级服务，确保所有终端设备能够持续获得病毒定义库的更新和最新的安全补丁。
2	提供不少于一年的软件许可更新服务，确保在此期间，所有终端防病毒软件保持正常运行，并能够实时检测和防御最新的病毒和恶意软件威胁。
3	对于重大安全威胁或爆发性病毒，需确保提供紧急更新服务，及时推送相关病毒定义库和安全补丁。
4	乙方需定期提供安全报告，包括病毒检测情况、威胁分析、风险评估及防御措施建议等。
5	提交详细的实施方案，包括防病毒软件的升级步骤、部署计划及时间表，确保在规定期限内完成所有升级运维工作。

交付物要求：

乙方需在服务期中每周提交以下交付物：

《防病毒运维周报》

（十二）移动端安全加固服务

乙方应在服务期内，向甲方提供两个移动端APP的代码安全检测和安全加固服务。按照国家相关法律要求，制定移动端软件隐私政策，确保移动端软件安全合规。

技术要求：

- 服务应包含 Android 端、IOS 端安全加固服务；
- 移动应用安全检测服务；
- 个人信息隐私合规双平台评估服务；

序号	移动应用安全加固服务要求
1	# 全量虚拟化技术：所有 dex 文件至少应进行函数抽取加密级防护。支持 DEX 全量虚拟化技术（ALL-VMP），能够将 DEX 代码的通过 DEX 虚拟化技术进行全量保护。支持对 SO 代码进行加密混淆，防止 IDA 的查看伪代码功能；支持 SO 动态清除技术，能够在 SO 执行过程中动态清除内存中的函数符号。（需提供证明函或截图证明并加盖乙方公章）
2	防篡改保护：加固后应用被保护内容与保护代码强耦合，被保护内容无法单独提取使用，防止应用被第三方篡改、破解，支持对 APK 内所有文件（DEX 文件、SO 库文件、H5 代码、assets 资源、res 资源、AndroidManifest 及签名）进行完整性验证，篡改后 APP 将无法正常运行。
3	数据防泄漏：加固后应用运行时内存数据不能被读取或修改，包括使用第三方工具进行内存数据读取或修改。当发生内存数据读取或修改攻击时，可以通过提醒用户或终止运行方式来阻止攻击。
4	# 支持语言：支持对 Object-C/Object-C++代码的源到源加固、支持对 Swift 代码的源到源加固，支持在不改变语义的前提下，通过控制流平坦化将控制流进行混淆处理。（需提供证明函或截图证明并加盖乙方公章）
5	反调试保护：防动态调试：加固后应用不能被第三方工具动态调试，运行逻辑和业务逻辑对外不可见，防止黑客通过工具（模拟器、修改器等）进行动态攻击；防进程调试：加固后应用不能被第三方工具进行进程调试。
6	# 动态检测：支持至少 18 项动态检测项，包括但不限于：篡改二次打包风险、应用签名未校验风险、数据库注入漏洞、动态调试攻击风险、http 报文信息泄露风险、界面劫持风险、本地端口开放越权漏洞、ContentProvider 数据泄漏漏洞、动态注入攻击、root 设备

	运行检测、模拟器运行检测等、Content Provider 导出组件目录遍历漏洞、SharedPreferences 文件中存储敏感信息、SQLite 数据库中明文存储敏感信息、Activity 导出组件拒绝服务漏洞、Service 导出组件拒绝服务漏洞、Broadcast Receiver 导出组件拒绝服务漏洞、Frida HOOK 运行风险。（需提供证明函或截图证明并加盖乙方公章）

服务频次：

服务期内提供两个移动端APP的代码安全检测和安全加固服务。

交付物要求：

乙方需在服务期结束前提交以下交付物：

《北京广播电视台APP加固报告》

《北京广播电视台APP安全检测报告》

《北京广播电视台移动APP个人信息评估报告》

（十三）信息系统等保测评服务

乙方应在服务期内，向甲方提供不少于2个三级系统的信息系统等级保护测评相关的安全咨询、安全评估、加固整改服务，并形成对应《等级保护测评报告》。

技术要求：

要求按照《中华人民共和国网络安全法》、《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019、《信息安全技术网络安全等级保护测评要求》GB/T 28448-2019、《信息安全技术网络安全等级保护测评过程指南》GB/T 28449-2019要求对甲方信息系统开展等级保护测评，定位网络安全现状与国家等级保护要求的差距，落实等级保护各项要求，提高网络安全总体水平，增加网络攻击防范能力，并编制形成《等级保护测评报告》。

为保证测试的公正和准确，乙方应对服务过程中使用的各种软件的版权负责。保证测试所采用的测试工具均需为正版测试工具，如果因此引起版权纠纷，由供应商承担相应责任。

服务频次：

服务期内，完成不少于2个三级系统的等级保护测评工作。

交付物要求：

乙方需在服务完成后 20 天内提交以下交付物：

《信息系统等级保护测评报告》

《信息系统等保测评差距分析报告》

《信息系统等级保护整改建议》

（十四）容器安全检测服务

乙方应在服务期内，向甲方提供不少于 150 点位的针对主机容器环境下的容器安全检测服务。按照国家相关法律要求，具备容器资产清点、容器风险检查、容器安全基线、容器入侵检测和响应、集群安全检测、异常行为检测、内存后门检测等能力，同时应提供容器安全统一管理能力。

技术要求：

服务范围：确保不少于 150 点位的容器环境安全合规。

详细技术要求包括：

序号	容器安全检测服务要求
1	# 部署模式：容器安全 agent 须能够与我单位已购青藤万相主机安全 agent 完成兼容性对接，实现主机和容器的统一安全管理，从而避免安装多个 agent 增加运维工作量（需提供承诺函）
2	# 资源限制：平台应限制客户端的资源占用，Agent 客户端的资源占用不应超过 1c1g。Agent 支持以非 root 权限方式运行。（需提供证明函或截图证明并加盖乙方公章）
3	通用功能：平台应具备对所有运行组件的自管理能力，支持在界面上显示其与服务端的通信状态，支持在产品界面上下载组件日志，对于异常组件提供删除探针、重启探针、停用探针等快速处置操作。能够对系统各运行组件（包含容器 Agent 等）自动化平滑升级。支持在产品界面管理客户端的安装和升级操作，支持在界面上配置组件安装所需要的配置，例如支持在界面上自定义命令空间、CPU、内存、Secret 等，并支持通过平台一键在集群中安装&升级客户端。产品应支持各组件的监控、告警能力，应能监控组件的资源占用情况，包括 CPU、内存、磁盘 IO 等的占用趋势；应当探针出现频繁离线、停用、卸载等异常行为时，应实时进行告警通知。
4	# 资产统计：支持自动获取集群中的容器资产，并自动关联容器所

	属的节点、所属集群、对应 pod、来源镜像信息，同时细粒度梳理容器中的进程、端口、数据挂载、网络、安装包、环境变量等信息。能够清点镜像资产，具体包括 Repository、Tag 、创建时间镜像大小、关联镜像、以及关联到镜像的风险信息。（需提供证明函或截图证明并加盖乙方公章）
5	应用风险：支持采用 POC 的漏洞验证的方式检测的容器中运行的应用漏洞是否真实存在且可被利用，例如 tomcat、redis 等，并且在页面上能显示详细的漏洞详情、POC 的执行结果、修复建议、CNVD 等信息
6	集群风险：支持 kubernetes 安全检测，并提供漏洞详情和修复建议。支持产品中集群风险检查规则开放展示，用户可查看检查项详情并自定义检查项启用/禁用状态。支持 docker 安全检测、Harbor 安全检测等，并提供漏洞详情和修复建议。支持产品中集群风险检查规则开放展示，用户可查看检查项详情并自定义检查项启用/禁用状态。
7	# 安全性：客户端具备手动降级机制，即当 Agent 出现异常时，允许通过产品前台，将 Agent 设置为停用模式、降级模式；当问题处理后，可通过前台，将其设置为正常模式。探针应具备自杀&重启机制，当 Agent 发现自身资源占用过大时，例如 CPU、内存等，Agent 进程会自杀重启。客户端不得修改服务器操作系统内核或驱动，并禁止采用抓包技术（需提供由国家信息中心软件测评中心颁发的评测报告）

服务频次：

服务期内，提供维保标准服务及产品规则库更新服务。

（十五）蜜罐服务

乙方应在服务期内，向甲方提供面向台内业务生产环境下的动态欺骗防御系统服务，按照国家相关法律要求，具备仿真、预警发现、攻击分析等能力。

技术要求：

详细技术要求包括：

序号	蜜罐服务技术规格要求
1	乙方所投设备为自有设备，1U 机架式设备、CPU≥8 核、内存≥32GB 内存、硬盘≥1TB 硬盘、标配千兆电口≥6 个、USB 口≥2 个、Console 口≥1 个、单电源 250W

2	支持 TRUNK 模式交换机旁路部署，不克隆系统，不采用引流，对网络带宽资源无占用，不改变用户网络拓扑进行部署；
3	支持配置 20 哨兵节点 100 个虚假仿真主机 IP 节点，每 IP 关联不同的硬件 MAC 地址；
4	# 支持自适应智能策略功能。保证每个仿真主机节点 IP 地址均能进行自适应的诱捕策略自动生成，无需逐个仿真主机节点进行静态诱捕策略配置(提供产品功能截图并加盖乙方公章)；
5	# 自适应智能策略支持同一个虚假仿真 IP 地址对不同意图攻击者生成不同诱捕策略(提供产品功能截图并加盖乙方公章)；
6	自适应智能策略功能支持策略记忆能力，对同一个攻击者 IP 的多轮不同顺序的端口扫描保持相同的端口开放格局
7	# 支持仿真主机节点动态漂移，定期自动更换每个哨兵节点的 IP 地址(提供产品功能截图并加盖乙方公章)；
8	# 内置仿真资源库，各类仿真资源可按需组合构成场景，仿真资源库内不同类型仿真资源数量不少于 100 种(提供产品功能截图并加盖乙方公章)；
9	支持溯源反制服务，包括：Linux 溯源反制、Windows 溯源反制；
10	支持配置多级管理员权限，不同权限管理员具备不同的系统管理权限范围。
11	支持多类型 WEB 应用仿真
12	支持常见数据库类型应用仿真
13	支持常见通用网络协议仿真与交互

服务频次：

服务期内，提供支持不少于配置100个虚假仿真主机的动态欺骗防御系统服务。系统的维保标准服务。