国专合同编号
17 12 22
170556

合同登记编号：

国家知识产权局专利局
网络安全运营服务项目合同

项目名称 ： 网络安全运营服务

项目编号 ： 17-2103

甲　　方 ： 国家知识产权局专利局

乙　　方 ： 北京中软泰和科技有限公司

签定地点 ： 北京

国家知识产权局专利局（以下简称“甲方”）和北京中软泰和科技有限公司（以下简称“乙方”）根据《中华人民共和国合同法》同意按下述条款和条件签署国家知识产权局专利局网络安全运营服务项目合同（以下简称“合同”）。

第一条　定义

除非根据上下文另有解释，本合同中使用的术语含义如下：

1. “合同”系指本文条款及其所有的附件、附录和上述文件所提到的构成合同的所有文件。

2. “合同价”系指根据合同规定乙方在正确地完全履行合同义务后甲方应支付给乙方的价格。

3. “软件”系指一个或多个能在控制器、处理器或其它硬件设备上运行的所有程序（包含相关的文档）。

4. “服务”系指根据本合同由乙方履行的任务和服务，包括但不限于集成、实施、试运行、验收、维护、培训、咨询、技术支持和项目管理等技术文件中所描述的活动。

5.“可交付物”系指根据本合同乙方应交付甲方的文件、文档和其它材料。

6.“天”系指日历天数。开始当天不计入，从次日开始计算。时限的最后一天是法定节假日的，以节假日次日为时限的最后一天。时限的最后一天的截止时间为当日 24 时。

7. “验收”系指甲方依据合同所规定的验收的程序和条件，对乙方提供的服务和可交付物进行检验和测试，以验证其是否满足本合同及合同附件的要求。

8. “项目”系指网络安全运营服务项目。

第二条 工作范围及服务时间、服务地点

1. 乙方根据本合同及附件的规定为甲方提供网络安全运营服务。

2. 本项目服务期为自合同签订之日起 24 个月。

3. 本项目服务地点为：北京市海淀区蓟门桥西土城路 6 号国家知识产权局

第三条 标准

本合同项下提供的网络安全运营服务应符合本合同中所述的标准。

第四条 合同价

1、本合同总价款为：大写（人民币）：壹佰壹拾柒万捌仟伍佰元整，小写：¥1,178,500.00。

2、甲方按以下进程分阶段向乙方支付上述款项：

A 首付款：合同签订后，按照甲方支付时间向乙方支付，计大写（人民币）：壹拾玖万伍仟柒佰 元整，小写：¥195,700.00 元；

B 初验款：合同签订后，服务期满 6 个月且初验合格后，按照甲方支付时间向乙方支付，计大写（人民币）：肆拾玖万壹仟肆佰 元整，小写：¥491,400.00 元；

C 尾款：服务期结束后进行项目验收，经甲方验收合格双方签署验收报告后，按照甲方支付时间向乙方支付，计大写（人民币）：肆拾玖万壹仟肆佰 元整，小写：¥491,400.00 元；

3、甲方应将价款支付至乙方提供的如下账户内：

账户名称：北京中软泰和科技有限公司

开户银行：北京银行中轴路支行

帐号：010 9036 1800 1201 0911 3169

若乙方支付信息发生变更，须提前 20 个工作日书面通知甲方。否则，由此造成延期支付的责任由乙方承担。

4、若甲方已经签署付款指令，但因非招标方流程等非人为原因和政府行为造成的延期支付，不视为甲方延期付款，甲方不承担违约责任。

5、甲方付款前，乙方应开具符合甲方要求的正式发票。乙方出示的发票应包含足够详细的内容，使甲方能够确定金额的准确性；如乙方提交的发票不合格，甲方可延迟付款。

6、如乙方根据本项目规定有责任向甲方支付违约金或其它赔偿时，甲方在

书面通知乙方后，有权从上述付款中扣除该等款项。

7、合同价已包含乙方履行本合同全部义务所应获得的价格，包括但不限于：服务费用、乙方不得以任何理由要求增加费用，甲方书面同意的除外。

8、除非双方另行约定，合同价已经包括所有完成开发任务所需要的材料、人工费及销售、使用、服务、增值或类似的税项。甲方可以根据中国法律的要求，从支付给乙方的款项中代扣所应缴付的相应税款，为此，甲方应向乙方提供缴税凭证。

9、本合同涉及的任何价格调整，均应以合同价为基价进行。

第五条　甲方义务

1、甲方或甲方委托方指派的代表作为甲方的项目经理，与乙方进行及时的联络并监督、协调服务的执行情况。

2、在网络安全运营服务中发现问题，及时与乙方联系，协助乙方解决相关问题。

3、配合乙方协调、安排甲方参与本项目的技术、业务人员，确保有足够的时间投入本项目的服务中。

4、按期支付费用。

第六条 乙方义务

1、及时履行合同义务和项目技术方案中规定的具体义务。

2、根据本合同的条款和条件，满足甲方在技术需求和业务需求中的要求，并提供网络安全运营服务项目中具体描述的可交付物。

3、根据本合同及其附件中确定的时间表提供可交付物和咨询服务。

4、负责建立日常工作制度，并进行项目的日常管理工作，并对其成功予以保证、对其实施负担全部责任。

5、根据甲方要求，在规定的时间内安排相应人员进入甲方指定的工作场所进行维护服务，遵守甲方制定的工作规定和工作制度。乙方安排的人员在工作期间，必须服从甲方的工作规定和安全管理制度，包括但不限于：国家知识产权局电话管理办法、国家知识产权局固定资产管理办法、国家知识产权局自动化设备管理规定、网络监控管理办法。如果乙方工作人员不服从甲方管理，造成严重后

果，甲方有权解除合同并提出索赔。

第七条　保密

1、乙方承诺以最严格的保密方式保存和维护从甲方或甲方代表获得的保密信息，未经甲方事先书面同意，不得向任何第三方披露。保密信息包括但不限于本项目、规格、计划、设计、软件及开发资料、数据、图纸、式样、样本或甲方为上述内容向乙方提供的任何其它资料。

2、乙方应保证其雇员：

A 只有在为了本项目的目的而必须知道保密信息的情况下，才允许获取从甲方或甲方代表获得的任何保密信息；

B 必须了解本项目规定的保密要求并与乙方签订保密协议；

C 不得造成或允许向任何第三方透露保密信息。

3、未经甲方书面许可，乙方透露或使用了保密信息，应当在不损害甲方其它利益的情况下，尽一切努力协助甲方收回保密信息，防止使用、传播、出售或以其它任何方式处置该保密信息。

4、本项目终止后 3 个工作日内，乙方应向甲方交还其获得的保密信息，不得以任何方式进行复制留存。

5、本项目有效期间及其后的十年内，本条款的规定仍对乙方发生效力，不因本项目的终止而失效。

第八条　技术支持与服务

1、乙方应针对我局项目特点，针对性的提供详细网络安全运营服务的需求分析及可行、合理的服务方案。

2、乙方应对各详细服务技术要求逐一响应并提供详细、可行、合理的技术方案。

3、乙方须设立有客户服务响应中心为我局提供方便查询的全天候运营 400 或 800 热线电话服务，同时提供传真、EMAIL 服务。

乙方应指派专人作为客户经理负责甲方的服务，以便能够提供更好的、更及

时的提供服务；

远程技术咨询：对于日常中碰到的有关安全设备技术、业务的一般性问题，乙方须提供咨询服务，尽最大努力，最大限度满足招标人的需求；可通过电话、传真、EMAIL 向乙方提出服务申请。

现场技术支持：对于通过电话支持服务、远程服务、驻场工程师都不能解决的问题，乙方须提供及时响应并安排经验丰富的技术支持工程师在规定时限内到达现场并提供现场支持。

4、乙方统一负责提供以下网络安全运营服务所需的技术支持和安全运营咨询服务，主要包括驻场服务，边界安全基线服务，网络安全日志分析服务，安全监控服务，特殊时期保障，预防性维护，季度交流，服务报告等。

5、服务报告与例会，乙方建立运维文档与运维日志并在每月向我局提供上月度《网络安全运营月度简报》，以便我局全面准确的了解上月网络安全运营服务实施情况。

乙方应定期向我局提供《季度网络安全运营服务总结报告》，以便我局全面准确的了解网络安全运营服务实施情况。

我局每个季度组织召开双方参与的网络安全运营会议，乙方汇报上个季度网络安全运营情况和合同执行情况，汇报遗留问题处理情况，提出对网络安全加固防护建议，双方共同确定下一步的网络安全运营工作安排。

第九条 索赔

1、若乙方违反本项目的约定，例如由于乙方原因导致项目偏差，且甲方根据本项目关于人员承诺、人员变更、测试、安装、调试、试运行、验收和项目保证期等相关条款的规定提出了索赔，甲方有权要求乙方赔偿。

2、若发生“技术支持与服务”“履约延期”和上述情形之外的任何违约时，违约方在接到对方关于违约的通知时，均应当就每一项违约向对方支付相当于当期服务金额 5%的违约金。当构成严重违约时，对方可以单方面决定解除或终止项目履行，违约方同时还应当承担违约及/或赔偿责任。

3、如果在甲方发出索赔通知后 30 日内，乙方未作答复，上述索赔视为已被

乙方接受。若乙方未能在甲方发出索赔通知后30日内或甲方同意的延长期限内，按照甲方同意的上述规定的任何一种方法解决索赔事宜，甲方将从应付款中扣除索赔金额。

第十条 履约延误

1、乙方应按照本合同有关条款和条件及时且合格地向甲方交付可交付物和提供服务。

2、乙方延误或部分延误交付可交付物或服务的，在原定时间的15日前以书面形式将延误的事实、可能延误的时间和原因通知甲方，并提供更新的项目计划，阐述由于延误对整个项目的影响。甲方在收到乙方通知后，将有权选择延长部署时间、或收取延误赔偿费、或解除项目。

3、乙方履约延误的，应向甲方支付延误违约金。每延误一周的违约金为合同总价款的百分之一(1%)，不足一周按一周计算。乙方履约延误超过30天，甲方有权单方解除本合同。

4、甲方按本条规定要求乙方承担责任外，并不影响甲方继续以其它任何形式要求乙方承担违约责任和赔偿。

第十一条 人员变更

1、乙方不得在履行项目期间更换项目经理，若因不可抗力，必须变更时，乙方选派一名具有同等或更高资历的人员进行替换。

2、乙方不得在履行项目期间更换项目主要技术负责人，若因不可抗力，必须变更时，乙方应选派一名具有同等或更高资历的人员进行替换。

3、若甲方发现乙方项目经理或主要技术负责人存在以下问题，甲方有权书面要求投标方予以更换：

A 该人员被发现犯有严重的错误或涉嫌犯罪行为；

B 甲方有理由认为该人员能力与表现无法胜任承担的工作任务。

乙方在收到甲方书面通知后，必须及时更换该人员。4、新更换人员的资历应事先得到甲方认可。乙方不得因人员的变更影响项目的价格及项目履行期限。

第十二条 伴随服务

1、乙方提供下列服务，包括本项目规定的附加服务：

A、在甲方要求的合理期限内对所提供的规范和数据标准进行调整。

B、乙方仅对甲方指定的人员进行培训。

2、乙方提供本项目中规定的所有服务，为履行要求的伴随服务的报价或双方商定的费用已包括在项目价中。

第十三条 乙方保证

1、乙方保证，不会因乙方问题导致甲方的硬件故障、系统瘫痪、数据丢失等情形。

2、乙方保证，乙方始终保护系统和甲方的其它财产不会因为乙方故意或过失的行为或疏忽而受到毁坏、损害或造成损失。

3、根据甲方要求，在规定的时间内安排相应人员进入甲方指定的工作场所进行服务。乙方进场服务产生的费用由乙方自行负责。乙方安排的人员在工作期间，必须服从甲方的工作规定和安全管理制度，包括但不限于：国家知识产权局电话管理办法、国家知识产权局固定资产管理办法、国家知识产权局自动化设备管理规定、网络监控管理办法。如果乙方工作人员不服从甲方管理，造成严重后果，甲方有权解除项目并提出索赔。

第十四条 合同修改

以维护和兼顾各方的利益和信息系统的最优化为原则，在本项目的基本范围内，甲乙双方均有权在履行本合同的过程中适时地提出变更、扩展、替换或修改本项目的某些部分，包括但不限于项目管理范围的调整、技术参数的提高或提升、交付或实施的时间与地点的改变等。为此，双方同意：

1、甲方可以要求对本合同进行修改。所有的修改要求都应以书面形式提交。甲方将准备一份书面的修改备忘录以说明所要求的更改，并列出对技术文件条款的任何修改。乙方应在 3 日内对此做出书面回应，其内容包括详细的该修改对合同价格、项目交付日期、项目技术参数的影响和变化以及对合同条款的影响等。

2、甲方收到乙方的上述回应后，应在 3 日内以书面方式通知乙方是否同意

和接受乙方的上述回应。如果甲方接受乙方的上述回应，则双方另行对此修改签署予以确认，乙方则按修改后的约定履行本合同。

如甲方对乙方的回应不同意（如对价格或交付日期的变化等），甲乙双方应进行协商，如协商成功则按协商执行；如协商不成功应采用本合同“争议的解决”，在协商期间乙方应安排人员执行甲方的修改。

3、如乙方提出项目的部分修改建议，乙方应同时以书面形式详细阐明该变更对合同价格、项目交付日期、项目技术参数的影响和变化以及对合同条款的影响等。

4、甲方收到乙方的上述修改建议后，应在 3 日内以书面方式通知乙方是否同意和接受乙方的上述修改建议。如果甲方接受乙方的上述回应，则双方另行对此修改建议予以确认，甲乙双方则按修改后的约定履行本合同。如甲方不同意乙方的上述建议，双方仍按原合同执行。

5、所有的修改应在双方签署书面的修改备忘录时生效。修改备忘录将变更或取代有关的技术文件中或先前的任何修改备忘录中所有不一致的条款。

6、任何对合同条件的变更或修改均须双方签订书面的修改书。

第十五条 知识产权

1、本项目涉及的全部及/或任何部分的相关知识产权、相关权益，包括本项目相关的且为履行本项目合同而新形成的商业秘密信息、技术资料和技术诀窍等，均归招标方所有。

2、投标方有不可争议的义务确保招标方依据本项目所获得的知识产权在中国境内（香港、澳门、台湾地区除外）不存在任何瑕疵并且可以不受限制地行使相关权利，包括各项延伸权利。若因此发生任何争议均应由投标方独自承担全部及/或任何责任，包括但不限于承担其自身及招标方为解决任何争议及/或瑕疵及/或缺陷所应当或所需要支付的一切相关及/或由此引起的费用。

3、 招标方将拥有其在本项目项下所从事的所有工作（包括各类纸质文档，电子文档及其它可交付物）中所包含的或与之相关的全部版权、专利权、商业秘密、商标权和其它知识产权以及所有权和其它权益。

4、在本项目合同生效日前业已存在的版权及其它知识产权和技术秘密应属于本项目合同生效前即拥有该等权利的一方或与该方有协议关系的第三方。任何一方均无权凭借本项目合同取得另一方此前所拥有且根据本项目合同不应被合理的推论为其已经同意转移的版权、专利权、商业秘密、商标权或其它知识产权的所有权。

第十六条 不可抗力

1、合同任何一方由于受诸如战争、严重火灾、洪水、台风、地震等不可抗力事件的影响而不能执行合同时，履行合同的期限应予以延长。延长的期限应相当于事件所影响的时间。不可抗力系指双方在签署合同时所不能预见的、不能避免并无法克服的客观情况。

2、受不可抗力事件影响的一方，应在不可抗力事件发生后尽快用电报、传真或电传通知对方，并于事件发生后 14 天内将有关机构出具的证明文件用特快专递或挂号信寄给对方予以确认。

3、若不可抗力事件的影响持续 30 天以上，甲方有权确定是否延期履行或终止合同。

第十七条 争议的解决

如因履行本合同发生争议，甲乙双方应尽量协商解决。协商不成时，任何一方均有权向甲方住所地人民法院提起诉讼。

第十八条 适用法律

本合同适用中华人民共和国的法律。

第十九条 通知

1、任何通知应以快递、电报、电传或传真的方式发送至合同中载明的地址，快递、电报、电传或传真须经对方签收。

2、通知以送达日期或通知书载明的日期为生效日期，两者中以日期在后者为准。

甲方：国家知识产权局专利局　　联系人：林琳

地址：北京市海淀区西土城路6号　　邮编：100088

电话：010-62083435　　传真：010-62083147

乙方：北京中软泰和科技有限公司　　联系人：李文权

地址：北京市海淀区中关村软件园内软件广场C座云基地2层　　邮编：100094

电话：010－56730980　　传真：010－59403265

第二十条 合同生效

本合同经甲、乙双方法定代表人或授权代表签字并盖章后生效。

第二十一条 其它约定事项

1、本合同未尽事宜，双方另行协商并签订补充协议明确。

2、本合同所有附件为合同的有效组成部分，与本合同具有同等法律效力。

3、本合同附件为：

《附件A:网络安全运营服务方案》；

《附件B保密责任书》；

《附件C：项目责任书》

4、本合同一式柒份，甲方执陆份，乙方壹份（正本），每份具有同等法律效力。

甲方：国家知识产权局专利局　　**乙方：北京中软泰和科技有限公司**

法定代表人或授权代表：　　**法定代表人或授权代表：**

日期： 2017.12.22　　**日期：** 2017.12.18

网络安全运营服务方案

北京中软泰和科技有限公司

2017 年 12 月

目录

1 项目概述

1.1 项目背景

随着国知局信息化建设脚步不断的加快，国知局内外网相关对外提供网络安全防护设备也不断的增多，目前国知局内外网涉及多种安全设备类型，包括：DDoS 5 台，防火墙 21 台，IDS 8 台，IPS 18 台，WAF 8 台，安防及入侵检测 7 台，安全配置核查系统 8 台，漏扫 9 台，数据库及业务审计 3 台，其它安全设备 15 台等安全设备，共计 102 台。涉及几十个业务系统。一旦发生业务系统重要数据被攻击或窃取等重大突发信息安全事件，将会极大的损害国知局的公信力和公众的利益。因此，做好内外网安全运营保障尤为重要。

为了及时发现国知局安全防护体系、安全防护工具、安全防护运维中存在的安全风险并采取防范措施，现启动网络安全运营服务项目。

本项目的总体目标是：通过网络安全运营服务，及时发现国知局安全防护体系、安全防护工具、安全防护运维中存在的安全风险并采取防范措施，一旦发现信息安全风险问题能够后及时获知并通知相关系统管理员，以便及时整改，保障国知局网络安全防护设备的安全运行，为业务系统信息安全保驾护航。

1.2 服务目标

中软泰和将通过对国知局内外网相关对外提供网络安全防护设备实施网络安全营服务，从而协助甲方信息化管理部门掌握其管辖范围内的信息系统安全防护设备进行安全基线检查、网络安全日志分析、安全监控，同时通过此服务发现在网络安全运营工作中存在的各种问题并提出整改建议，保障国知局网络安全防护设备的安全运行，为业务系统信息安全保驾护航。具体服务目标为：

1) 定期采用人工检查用表、脚本程序或基线扫描工具等对评估目标范围内的安全设备进行系统的策略配置、服务配置以及安全系统软硬件升级、更新情况，是否存在后门等内容进行检查的服务并处理。

2) 定期分析局内外网网络安全设备日志信息，形成网络安全日志分析报告，

提供网络安全设备安全加固建议和网络安全防护建议，提高国知局网络安全保障能力。

3) 对局外网出口安全设备进行有效监控，结合网络安全威胁情报，对网络安全事件处理提供分析处理服务。

4) 针对突发的信息安全事件提供应急响应服务，协助解决安全事件；

5) 重要时期及特殊情况下要加强保障，提供定期信息安全工程师到现场进行网络安全运营服务数据采集、评估、报告、保障。

1.3 服务内容

1.3.2. 服务对象

国知局目前内外网涉及多种安全设备类型，包括包括：DDoS 5 台，防火墙 21 台，IDS 8 台，IPS 18 台，WAF 8 台，安防及入侵检测 7 台，安全配置核查系统 8 台，漏扫 9 台，数据库及业务审计 3 台，其它安全设备 15 台等安全设备，共计 102 台。所需运营服务各类安全防护设备分布在内网和外网相关 7 个安全防护区域，安全防护涉及几十个业务系统。

具体设备清单如下：

序号	设备名称	型号	数量
1	入侵检测	ICEYE-1200P-04	1
2	入侵检测	ICEYE-200P-02-B	1
3	入侵检测	ICEYE-1200D-02	2
4	入侵检测	ICEYE-1200A-02	3
5	远程安全评估	AURORA-200-U	2
6	应用防火墙	ICEYE-WAF-1000-04-B	2
7	远程安全评估	AURORA-600	2
8	安全中心	SG-2000	2
9	安全配置核查系统	SAS-1000	2
10	漏洞扫描	RSAS-S	4
11	抗拒绝服务系统	ADS-4000	2
12	入侵防御	NIPS-2000A-V	2
13	应用防火墙	ICEYE-WAF-1200	3
14	安全配置核查系	BVS-S	1

	统		
15	入侵防御	NIPS-1200A	3
16	入侵检测	NIDS-1200A	2
17	安全配置核查系统	SAS-1000A	5
18	应用防火墙	WAF-P1600A	3
19	漏洞扫描	RSAS M	3
20	入侵防御	NIPS 4000A	2
21	入侵防御	NIPS 1200A	2
22	防火墙	NGFW4000-UF	2
23	入侵防御	NIPS NXS	1
24	日志收集与分析	TopAud	1
25	下一代防火墙	NF NX5	2
26	入侵防御	NIPS-600A	2
27	抗拒绝服务系统	ADS-200A	1
28	安全中心	SG-1200A	1
29	入侵检测	ICEYE-610P-03-B	1
30	入侵防御	NIPS N2000	2
31	入侵防御	NIPS-N2000A	1
32	入侵检测	NIDS-2000A	1
33	安全配置核查系统	SAS-H1100A	1
34	抗拒绝服务系统	COLLAPSAR-200-50-B	1
35	漏洞扫描	RSAS-X	1
36	入侵检测	NIDS-N2000A	2
37	入侵防御	NIPS-NX3-N2000A	2
38	入侵防御	NIPS-NX3-ZN2001A	1
39	远程安全评估	AURORA-200-64	1
40	入侵检测	NIDS-NX3-ZN3001A	1
41	防火墙	SecGate 3600 X300-TG300M2	2
42	防火墙	SecGate 3600 G7-5966-MP	2
43	防火墙	NISG 600 Net Eye	2
44	移动加密	SJJ0923	1
45	防火墙	NS-Dptech FW1000-GA-AC	2
46	业务审计	SecFox-NBA-LR3	2
47	防火墙	SecGate 3600 G30-6866	2
48	数据库审计	LA-DT-1000B	1
49	防火墙	SecFox3600-LAS-R31	1
50	安全网关	U4-1260A(MP)-H1.7	2
51	防火墙	SecGate 3600 A3000-T500P	2
52	防火墙	防火墙 Power V-6400U	2
53	漏洞扫描	漏洞扫描 CNS-GU256	1
54	入侵检测	IDS NS2200	2

55	抗拒绝服务系统	DDOS Leadsec-Guard-3200C	2
56	防火墙	防火墙 Power V-4400C	2

注：关于服务期内新增的安全设备，中软泰和可免费提供运营技术支持服务（不包括备件服务）。

1.3.2. 服务内容

序号	服务类型	服务内容
1	边界安全基线服务	采用人工检查用表、脚本程序或基线扫描工具等对评估目标范围内的安全设备进行系统的策略配置、服务配置以及安全系统软硬件升级、更新情况，是否存在后门等内容进行检查的服务并处理。
2	网络安全日志分析服务	定期分析局内外网网络安全设备日志信息，形成网络安全日志分析报告，提供网络安全安全加固建议和网络安全防护建议，提高国知局网络安全保障能力。
3	安全监控服务	对局外网出口安全设备进行有效监控，结合网络安全威胁情报，对网络安全事件处理提供专家分析处理服务。

1.4 服务时间

中软泰和为甲方提供自合同签订之日起 24 个月的网络安全运营服务。

1.5 服务地点

中软泰和将按照招标要求提供服务，并且在服务期内提供甲方需要的地点服务：北京市海淀区蓟门桥西土城路 6 号国家知识产权局。

2 网络安全运营服务方案

2.1 服务原则

为甲方提供服务时中软泰和将严格遵循以下几项服务原则：

1、合法性原则

在提供服务时，符合国家信息安全法、信息系统等级保护等相关法律标准关于网络安全应急响应的规定。

2、规范性原则

依照规范的操作流程进行安全运营相关安全基线检查、安全日志分析、安全监控服务，所有服务人员均需对各自的操作过程及结果进行详细的记录，并按照规范的报告格式提供各类服务文档。

3、最小影响原则

网络安全运营服务工作尽可能减少对原系统和网络正常运行的影响，尽量避免对原网络运行和业务正常运转产生显著的影响，包括：系统性能明显下降、网络阻塞、服务中断等。如无法避免，必须在服务前向甲方相关人员说明情况。未得到甲方的批准，不得擅自进行任何服务操作。

4、保密性原则

对于在服务过程中获知的任何关于甲方的系统信息承担保密的责任和义务，不得泄露给任何第三方的单位或个人，不得利用这些信息进行侵害甲方的行为，每个服务人员均签订保密协议保证服务的保密性原则。

2.2 服务方案

通过认真阅读国家知识产权局专利局网络安全运营服务项目(招标编号：17-2103)的招标文件，以及通过与客户单位管理人员、技术人员交流，中软泰和深刻地体会到本项目在客户日常运营中的重要性，中软泰和为保障国家知识产权局专利局网络安全环境系统安全防护等关键设备提供专业的网络安全运营服务，确保系统正常运行。

中软泰和统一负责提供以下网络安全运营服务所需的技术支持和安全运营咨询服务，主要包括驻场服务，边界安全基线服务，网络安全日志分析服务，安全监控服务，特殊时期保障，预防性维护，季度交流，服务报告等多方面工作内容。

2.2.1 安全资产梳理服务

根据本项目服务要求，在签定合同后，服务开始后第一季度内对局方安全资产调查并记录服务范围内各设备和系统版本的种类、型号、功能、物理位置、端口对应情况、部署情况等资产详细信息梳理和安全运营风险评估，提交《安全资产信息表》、《安全风险评估报告》、《网络安全整改建议》。

针对此项目要求我司指派不少于 2 名二线安全技术、2 名安全管理咨询专家到现场资产梳理及网络安全运营风险评估服务。

服务期内专家现场服务时间不少于 120 人天。

2.2.2 安全设备档案管理服务

中软泰和将利用资产调查的数据进行安全设备设备建档，绘制网络拓扑，统计信息点分布以及各安全硬件设备和软件系统的数量、拓扑位置、用途等信息；

安全设备档案文件包括不限于：

a) 设备信息，上线时间，负责人等运营管理信息；

b) 各安全硬件设备和软件系统的数量、拓扑位置、用途等信息；

c) 安全硬件设备和软件系统的版本及补丁更新信息；

d) 安全设备运行状态信息；

e) 安全设备运行性能信息。

f) 安全设备维护变更等信息；

每月度更新并提交《安全设备档案》。

2.2.3 安全基线检查服务

安全基线是保持信息系统安全的机密性、完整性、可用性的最小安全机制，是系统的最小安全保障，是最基本的安全运行要求。

安全基线最根本的目的是保障业务系统的持续稳定的安全运行，使业务系统

的运行风险维持在可控的范围内，为了避免人为疏忽或错误、或使用默认的安全配置，给业务系统安全造成风险，而制定的安全检查标准，并且采取必要的安全检查措施，使业务系统达到相对的安全指标要求。

根据此项目的要求，中软泰和提供定期通过人工检查用表、脚本程序或基线扫描工具对评估目标范围内的安全设备进行系统的策略配置、服务配置及安全系统软硬件升级、更新情况，是否存在后门等内容进行检查的服务。

服务标准

服务名称	服务标准
安全基线检查	每月第三周开展检查服务。每次安排不少于 3 名安全技术专家到现场服务，且每次现场工作时间不得少于 5 个工作日。
交付物	月末 28 号提交《月度安全基线检查报告》

2.2.4 网络安全日志分析服务

根据用户实际需求，提供定期分析局内外网网络安全设备日志信息服务，形成网络安全日志分析报告，提供网络安全安全加固建议和网络安全防护建议，提高局方网络安全保障能力。

日志获取及分析

通过登录各类评估目标安全设备，提取日志数据进行人工安全分析，可以对客户系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结参考。安全日志：记录服务器、防火墙等设备的日志，供安全审计系统使用，用于监控系统安全、进行可信取证等。

服务标准

服务名称	服务标准

网络安全日志分析服务	每月 25 号（如遇法定假日，按正常工作日顺延）对服务范围内的安全设备日志进行采集并进行专家分析。 每月度最后一周结合定期的外网安全设备日志与安全事件分析，为局方提供网络安全加固建议或网络安全防护建议。现场服务结束后 3 个工作日内提交《网络安全加固防护建议方案》。
交付物	每月 1 号提交上月度《网络安全日志分析报告》

2.2.5 安全监控服务

根据局方实际要求，局外网出口安全设备进行有效监控，定期通过人工或监控系统对服务范围内各设备的运行状态（如：CPU 利用率、内存利用率、磁盘利用率、端口流量、报警信息等关键工作指标）进行例行监控，通过人工方式对异常事件进行建档和归类（如：DOS 攻击、SQL 注入攻击等异常事件），生成《异常事件统计表》，统计表应包含但不限于：攻击类型、攻击次数、源 IP 地址、目标 IP 地址、攻击时间等内容；对于异常攻击 IP 进行合理的访问限制。

服务标准

服务名称	服务标准
安全监控服务及交付物	每天定点进行监控数据采集并记录，生成《安全监控数据统计表》； 每周提交《安全监控周报》； 第月提交《安全监控月度报告》； 每月 25 号（如遇法定假日，按正常工作日顺延）结合网络安全威胁情报对《安全监控数据统计表》进行专家分析并提供处理服务，输出《安全监控分

	析报告》； 网络安全事件分析处理服务是按局方要求指派二线安全专家到局方现场安全设备运行监控数据深度分析服务。结合网络安全威胁情报，对网络安全事件处理提供分析处理服务。服务时间每月不少于 5 人天。每次现场服务结束后 3 个工作日内提交《安全事件处理处理报告》。

2.2.6 特殊时间安全值守服务

在遇到一些特殊时间段，如：重大节假日（春节、国庆、劳动节、元旦等）、国际会议、国家军事、政治活动、系统升级等对系统要求较高的重要时段，及客户认为有必要的时间段，中软泰和将安排经验丰富的用户认可的至少一名二线安全服务工程师进行 7*24 小时现场不间断现场安全值守服务。遵照用户工作时间，服务内容含项目范围内涉及工作项。服务期内，除非取得用户书面同意，中软泰和提供的专职驻场工程师人员不得更换和撤离。

服务标准

服务名称	服务标准
特殊时间安全值守服务	服务期内二线安全服务专家现场安全值守服务时间不少于 480 小时。

2.2.7 安全事件保障支持服务

针对本项目我公司设立 7*24 小时报修热线服务和指定工程师报修服务，确保全年 7*24 小时的故障响应。

7*24 小时服务热线：400-875-8080 （7*24 小时）

专职项目经理手机：18611397985

如出现任何问题和故障，客户认为有必要中软泰和技术人员到现场支持时，我方将有限指定项目实施经验或维护经验的资深技术人员到现场支持，并按照客户时间要求感到现场，进行故障的处理。

如局方认为有必要指定某特定技术人员或者专家到现场支持时，我公司也将尽力满足客户要求，予以支持。

服务名称	服务标准
安全事件保障支持服务	如遇到网络与安全有关的紧急突发事件、网络入侵、拒绝服务攻击、网络病毒传播爆发等，中软泰和派出专业的信息安全工程师，快速响应，远程协助或到现场解决安全问题，远程响应时间为 15 分钟，现场响应时间为 1 小时到现场，4 小时排除故障，恢复正常。
交付物	当发生安全事件时，中软泰和应按安全事件响应时间进行有效响应，并对安全事件进行分析，在安全事件发生后 3 个工作日内提交《安全事件支持服务报告》。

2.2.8 项目配合服务

根据此项目具体需要，当局方在实施重大项目，如系统切换、系统升级、机房搬迁、安全测评及改造等时，需要我司配合或协助，我司积极响应及时指派资深支持人员现场协助及指导，提供各种必要的现场技术支持。

服务标准

服务名称	服务标准
项目配合服务	根据此项目具体需要，当局方在实施重大项目，如系统切换、系统升级、机房搬迁、安全测评及改造等时，需要我司配合或协助，我司积极响应及时

	指派资深支持人员现场协助及指导，提供各种必要的现场技术支持。

2.2.9 安全运营咨询服务

中软泰和坚持一切为了客户的服务理念，秉承客户数据安全和业务安全第一的原则，凭借多年以来协助客户实施信息安全管理、安全技术应用的大量经验，为您提供全方位的网络安全运营咨询全服务。

服务标准

服务名称	服务标准
项目配合服务	根据此项目具体需要，当局方在实施重大项目，如系统切换、系统升级、机房搬迁、安全测评及改造等时，需要中软泰和进行安全技术或安全运营管理咨询支持，中软泰和积极响应及时指派资深安全咨询人员现场提供各种必要的现场咨询服务。

2.2.10 工程师驻场服务

中软泰和在服务期内至少指派2名专业信息安全维护工程师提供5*9驻场服务，工作时间与国知局相同，不得迟到和早退，驻场工程师应严格遵守国知局工作管理制度，有相关的专业认证，对应的技术水平可以满足信息安全整体运维的要求以及需要满足国知局的保密要求，需要接受国知局定期的考核和评价，对不满足要求的工程师，国知局有权提出更换。

驻场工作服务内容：

1） 技术支持：负责发现的问题修改以及完善、同时验证问题的修改情况；中软泰和应按国知局要求及时完成安全防护设备的升级和打补丁工作，协调各方完成产品升级，并生成《技术支持事件跟踪表》提交给甲方。

2） 定期主动性预防工作：每周对运营范围内的目标设备进行深度健康巡

检，巡检项包括不限以下指标：CPU利用率、内存利用率、磁盘利用率、端口流量、报警信息、运行log、防护策略等关键工作指标；输出《巡检报告》并提交给甲方。

3） 定期安全防护设备运营日志分析：每周对运营范围内的目标设备进行日志采集并进行初步分析，如遇有安全事件或国知局管理规范中需要关注的情形出现应及时报告国知局项目接口人；

4） 安全事件响应：如有安全事件发生，应按照应急预案进行及时有效处理，保障系统安全运行；

5） 协助国知局进行网络安全监控运营：对现有安全防护设备进行运营管理，及时掌握设备的可用性情况和健康状况，从而保证安全防护设备的可靠、高效、持续、安全运行。监控数据应包括但不限于运行状态、故障情况、配置信息、可用性情况及健康状况性能指标；

6） 网络安全运营流程执行：协助国知局对网络安全相关各流程的执行、流程点监控报告等，保障安全运营流程执行的有效性。

交付物

《技术支持事件跟踪表》

《巡检报告》

2.2.11 服务报告与例会

服务开始前，我司将与用户协商确定服务实施计划，并提供《服务计划书》；

每次故障解决后，我司将于三个工作日内提供详细的《设备故障处理分析报告》；

设备变更或重要事件支持结束后，我司将于三个工作日内提供《设备变更处理报告》或《重要事件支持报告》；

每次季度服务结束后，我司将按要求提交《季度服务总结》。季度服务总结：包括不限于内容服务统计、重点服务说明、本季度所产生的故障总汇、本季度更换总汇及小结。

我司项目经理将定期对客户进行走访，调查客户满意度及对服务改进的要求，并提交《用户访问备忘录》；

服务标准

服务名称	服务标准
服务报告与例会	建议运维文档与运维日志； 每月 3 日前向局方提供上月度《网络安全运营月度简报》，以便局方全面准确的了解上月网络安全运营服务实施情况。《网络安全运营月度简报》内容包括但不限于以下内容： （1）上月度服务有关情况。包括安全事件分析处理、现场服务、远程支持以及电话支持的情况。 （2）驻场服务情况，分类统计有关驻场服务工作情况。 （3）月度安全日志分析。

每季度结束后的 5 个工作日内，向局方提供《季度网络安全运营服务总结报告》，以便局方全面准确的了解网络安全运营服务实施情况。

《网络安全运营服务总结报告》内容包括但不限于：

1) 服务情况的总结。对上个季度的网络安全整体运行情况进行总结，统计评估服务情况的内容；总结分析遗留问题处理情况 。
2) 季度网络安全日志分析总结；
3) 网络安全加固建议和网络安全防护建议；
4) 季度网络安全事件处理情况总结；
5) 计划执行分析。分析服务计划执行情况，对计划未执行项或未按时执行项进行原因分析，分析隐含问题。当出现服务质量问题及不符合合同约定的情况，则需提出分析报告和整改措施。
6) 问题分析。对服务过程中出现的未曾预见的问题，及时分析总结，给出

问题解决建议。

交流例会

局方每个季度组织召开双方参与的网络安全运营会议，中软泰和汇报上个季度网络安全运营情况和合同执行情况，汇报遗留问题处理情况，提出对网络安全加固防护建议，双方共同确定下一步的网络安全运营工作安排。

2.3 服务支持方式

2.3.1现场技术支持服务

中软泰和指派两名工程师 5×9 专职驻守国知局提供网络安全运营服务，严格按照甲方应急管理、运维管理制度和流程进行服务，日常工作时间与甲方相同。遇到重大国内、国际活动、会议、节假日，根据用户需要，提供临时现场值守服务。每日完成网络安全运营监控、检检查等服务内容。现场技术支持服务内容包含但不限于以下内容：

1) 技术支持：负责发现的问题修改以及完善、同时验证问题的修改情况；中软泰和应按局方要求及时完成安全防护设备的升级和打补丁工作，协调各方完成产品升级。

2) 定期主动性预防工作：每周对运营范围内的目标设备进行深度健康巡检，巡检项包括不限以下指标：CPU 利用率、内存利用率、磁盘利用率、端口流量、报警信息、运行 log、防护策略等关键工作指标；

3) 定期安全防护设备运营日志分析：每周对运营范围内的目标设备进行日志采集并进行初步分析，如遇有安全事件或局方管理规范中需要关注的情形出现应及时报告局方项目接口人；

4) 安全事件响应：如有安全事件发生，应按照应急预案进行及时有效处理，保证系统正常运营；

5) 协助局方进行网络安全监控运营：对现有安全防护设备进行运营管理，及时掌握设备的可用性情况和健康状况，从而保证安全防护设备的可靠、高效、持续、安全运行。监控数据应包括但不限于运行状态、故障情况、配置信息、可用性情况及健康状况性能指标；

6) 网络安全运营流程执行：协助局方对网络安全相关各流程的执行、流程点监控报告等，保障安全运营流程执行的有效性。

7) 对于通过电话支持服务、远程服务、驻场工程师都不能解决的问题，我司提供 7*24 小时响应并安排经验丰富的技术支持工程师在 2 小时内到达现场并提供现场支持。

服务流程：

对于出现的安全问题，我公司驻场工程师会及时收集问题症状及相关数据，根据观察到的数据和反映进行问题初步分析；并根据收集到的所有信息进行深度问题分析，确定问题根源、原因和影响，并提出问题解决方案或应对方案，必要时，提供问题解决测试方案并对测试进行现场技术支持。在问题确认解决后，提交所有问题管理文档：包括问题分析报告、问题解决方案、应对方案、测试方案和问题管理档案。

在问题解决期间，如现场工程师无法在有效时间内解决故障，可以通过我公司的故障升级机制，升级到更高级工程师协同解决。

故障排查及恢复

当出现故障时，我司马上安排二线安全专家与客户联系，了解客户的故障情况，先行提供远程故障信息收集、分析、初步定为排除工作，同时我们立即与现场服务工程师进行联动，将安全故障在第一时间内进行排除并处理。

我公司在接到故障处理申请时将采取双线支持的方式，来保证最大限度帮助客户解决故障。先行的远程技术支持由经验丰富的二线安全专家对故障进行提前预判，并在有条件情况下进行远程故障分析诊断，做出故障预判，当故障得到定位后，由现场服务工程师按二线专家的操作流程，尽快将故障消除。

二线安全专家将预判的结果告诉驻场服务工程师确认，现场服务工程师将现场情况告知二线工程师进行确认，我公司工程师将结合现场实际故障情况做出合理的解决方案，并有一线工程师配合二线工程师共同排除解决，直到系统恢复正常运行。

中软泰和公司为客户提供“7*24 小时”快速响应的电话支持和现场响应服务。客户可以随时随地得到中软泰和公司工程师的电话响应。一旦收到现场紧急服务请求，中软泰和公司工程师根据故障的级别用最快的方式抵达现场进行紧急故障处理。

2.3.2 远程技术支持服务

针对本项目提供电子邮件和电话两种远程技术支持方式，远程技术支持提供7X24 小时服务。远程技术支持服务内容包含但不限于以下内容：

1） 电话支持

中软泰和设立有客户服务响应中心。提供 7*24 小时 400-875-8080 热线电话服务，同时提供 7*24 小时传真、EMAIL 服务。

我司指派专人作为客户经理张婷婷（18510510069）负责甲方的服务，以便能够提供更好的、更及时的提供服务，提供 7*24 小时电话支持服务，以便甲方能够及时进行联系；

2） 远程技术咨询

对于日常中碰到的有关安全设备技术、业务的一般性问题，中软泰和须提供7*24 小时咨询服务，尽最大努力，最大限度满足国知局的需求；可通过电话、传真、EMAIL 向中软泰和提出服务申请。

2.4 服务团队

中软泰和为本服务项目建立专门的项目组，服务期内，项目经理原则上不做更换。本项目共 11 名项目成员，基本信息如表 3-1 所示。

表 3-1　项目组成员基本信息表

序号	人员信息	专业资格证书	本项目中担任职位
1	张婷婷		客户经理
2	谢清草	信息系统项目管理师	项目经理
		IT 服务项目经理认证	
		ITIL V3 Foundation 认证	
3	赵星晨	CISP 认证证书	驻场服务工程师
4	李坤恒	CISAW 认证证书	驻场服务工程师
5	雷　光	CISAW 认证证书	二线安全技术专家
6	王建龙	CISP 认证证书	信息安全管理咨询专家
7	郝卫军	CISP、CISSP、CISA 认证证书	信息安全管理咨询专家
8	国明慧		客户服务专员
9	赵鹤轩		质量专员
10	兰思宇		文档管理专员

3 项目验收

3.1 项目验收准入条件

1. 当服务期满 6 个月后进行项目初验；

2. 当服务期满 24 个月且全部完成服务内容后进行验收。

3.2 项目验收流程

1. 验收申请

   由中软泰和提交验收文档申请验收；

2. 验收评价

国知局依据中软泰和提供的服务验收文档，逐项检查各服务项目的完成情况，并进行评价。

3. 验收确认

验收报告以服务验收文档方式提供，双方签署书面验收意见。

4. 如验收结论为不合格，国知局有权暂不签署验收文档及支付当期服务费用，中软泰和应按照验收标准进行弥补、改进或完善，待国知局重新组织验收并且验收合格后，国知局再向中软泰和支付当期服务费用。如果中软泰和在国知局提出整改意见后的一个月内经改进仍达不到验收标准的，国知局有权终止合同并拒绝支付服务费用。

3.3 项目验收标准

1、 项目初验

当服务期满 6 个月后且按合同要求完成相应服务内容，乙方向甲方提供运维文档及运维日志。

验收报告以服务验收文档方式提供，双方签署书面验收意见，作为支付当期服务款的依据。

当服务期满 6 个月后进行项目初验时，中软泰和向甲方提供如下技术成果文档。

序号	文档名称	数量
1	**《服务初验报告》**	1
2	**《网络安全运营服务半年度总结报告》**	1

《网络安全运营服务半年度总结报告》内容包括但不限于：

1) 服务情况的总结。对半年度的网络安全整体运行情况进行总结，统计评估服务情况的内容；总结分析遗留问题处理情况 。

2) 半年度网络安全日志分析总结；

3) 网络安全加固建议和网络安全防护建议；

4) 半年度网络安全事件处理情况总结；

5） 计划执行分析。分析服务计划执行情况，对计划未执行项或未按时执行项进行原因分析，分析隐含问题。当出现服务质量问题及不符合合同约定的情况，则需提出分析报告和整改措施。

6） 问题分析。对服务过程中出现的未曾预见的问题，及时分析总结，给出问题解决建议。

2、 项目终验

服务期满 24 个月且按合同要求完成所有服务内容。乙方向甲方提供运维文档及运维日志。

验收报告以服务验收文档方式提供，双方签署书面验收意见，作为支付当期服务款的依据。

服务期满，项目验收时，中软泰和向甲方提供如下技术成果文档。

序号	文档名称	数量
1	**《服务验收报告》**	1
2	**《网络安全运营服务总结报告》**	1

《网络安全运营服务总结报告》内容包括但不限于：

1） 全部服务期内服务情况的总结。对上个季度的网络安全整体运行情况进行总结，统计评估服务情况的内容；总结分析遗留问题处理情况 。

2） 全部服务期内网络安全日志分析总结；

3） 网络安全加固建议和网络安全防护建议；

4） 全部服务期内网络安全事件处理情况总结；

5） 计划执行分析。分析服务计划执行情况，对计划未执行项或未按时执行项进行原因分析，分析隐含问题。当出现服务质量问题及不符合合同约定的情况，则需提出分析报告和整改措施。

6） 问题分析。对服务过程中出现的未曾预见的问题，及时分析总结，给出问题解决建议。

附件 B

保密责任书

甲方（国家知识产权局专利局）与乙方（北京中软泰和科技有限公司）于 2017 年12月18日签订国家知识产权局专利局网络安全运营服务项目合同，乙方承诺并遵守以下保密规定。

1 定义

保密信息：是指甲方拥有或持有的、项目活动中所披露的（或者乙方与甲方交往过程中所知悉的）符合以下条件之一的商业、经营、技术或其他信息：

（1）在甲方披露（或者乙方知悉）时标明为保密、专有（或有类似标记）的；

（2）乙方在为甲方提供服务的过程中获得的有关甲方的任何信息、数据、资料（不论是甲方提供或披露的还是乙方偶然获得的）以及因项目实施所取得的任何工作成果，均为保密信息；

（3）在保密情况下由甲方披露（或者乙方知悉）的；

（4）根据乙方合理的商业判断应理解为保密信息的；

（5）记载于保密信息传递单的；

（6）以其他书面或有形形式确认为保密信息的；

（7）从上述信息中衍生出的信息。

“保密信息”包括但不限于：本承诺书内容；由甲方或其关联机构在本承诺书签署前或之后披露给乙方或其雇员的，任何研发设计、产品设计理念/想法、产品及其规格、数据、模型、样品、草案等技术类信息；营销要求和策略、产品计划及价格、客户名单、甲方存货情况、甲方供应商名单、甲方已经或拟购买/销售的产品或服务的价格、公司业务发展可能方向、拟进入领域、有关甲方或其客户的资信情况试用过程中出现的问题以及解决方法、试用结果、涉及经营管理的制度与流程等经营类信息；其它甲方披露的需向第三方承担保密义务的信息。无论这些信息是以书面、口头、图形、电磁还是其他任何形式披露。

2 保证

乙方就本承诺书约定的保密信息保证如下：

（1）对本承诺书和相关附件，以及乙方以各种方式获悉的保密信息进行严格保密；

（2）乙方现行保密制度足以对保密信息进行保密；

（3）乙方不将保密信息披露（或者促使或允许他人披露）给任何人，但因工作需要而“必须知情”的下列人员除外：乙方直接参与项目活动的高级管理人员或雇员；或者经甲方事先书面认可的、且向乙方提供专业咨询的人士；或乙方的关联机构中直接参与项目活动的高级管理人员或雇员；

（4）乙方不将保密信息（也不会促使或允许他人将保密信息）用于项目活动目的之外的其他任何用途，包括但不限于：将此保密信息的全部或部分进行仿造、反向工程、反汇编、逆向推导；

（5）在保密信息披露时，如甲方已明确表示保密信息不得复印、复制或储存于任何数据存储或检索系统，乙方不得复印、复制或储存保密信息；

（6）在项目活动结束后或者经甲方要求时，乙方须把含有保密信息的所有记录或资料（无论是以书面、磁盘储存或是以其他形式保留的）交还甲方或删除，并且将促使他人将上述记录或资料交还甲方或删除；如甲方要求，乙方须向甲方书面保证已经将上述记录或资料全部归还或删除；

（7）应甲方要求，乙方须就甲方根据第三方许可而披露的保密信息的任何部分与甲方签署

其他有关协议；

（8）乙方须告知并有效约束本承诺书提及的人士承担与本承诺书规定相同的保密义务并签署不低于本承诺书保护程度的书面保密承诺书或承诺。甲方要求时，乙方应向甲方提供上述承诺书或承诺的文本。如上述人士越权使用或泄露保密信息，乙方与行为人承担连带责任。

（9）乙方保证不向本项目提供服务的乙方人员之外的其他人员（包括不为本项目提供服务的乙方人员，以及非乙方人员）披露本承诺书项下的保密信息。乙方应告知并采取必要的有效措施保证参与本承诺书项下服务项目之乙方人员履行本承诺书项下的保密义务。若乙方人员（乙方任何人员）违反本承诺书项下的保密义务或泄露本承诺书约定保密信息，视为乙方违反本承诺书，乙方应按照本承诺书约定向甲方承担全部责任。

（10）乙方保证：在项目通过验收之日，乙方须将甲方在项目实施过程中提供的相关信息和资料全部返还给甲方；未经甲方书面同意，乙方不得擅自留存、使用、参考和拷贝。

3 陈述

3.1 保密信息包含的所有权利、产权和利益都归甲方所有。除乙方按照本承诺书规定的方式和范围使用保密信息外，乙方未被授予任何明示或默示的关于保密信息的其他权利许可。

3.2 乙方明确承认：甲方并未向乙方担保其提供的保密信息目前或将来是真实无误的。

3.3 乙方违反本承诺书可能造成甲方（包括甲方关联方）不可弥补的损失，单独的金钱损害赔偿不能提供充分的救济。因此，针对乙方的违反本承诺书或可能违反本承诺书的行为，甲方有权在实施其他可行的救济手段的同时，向任何具有管辖权的法院寻求采取禁令性救济措施。

3.4 甲方向乙方披露保密信息的行为并不构成甲方将与乙方或其他实体进行任何商业合作的承诺；如果甲乙双方意欲建立任何商业合作关系，应另行签订书面协议。

4 保密期限

乙方应按本承诺书约定对保密信息持续地承担保密义务，除非（1）甲方以书面形式明确说明其披露的特定保密信息可不再保密，或（2）保密信息已被公众从公开途径获悉。

5 违反本承诺书的责任及权利救济

5.1 如乙方违反本承诺书约定的任何一项保密义务，每次违反时，甲方可要求按下列方式（几种方式同时适用）处理：

5.1.1 乙方应立即停止并纠正违反本承诺书的行为，消除因违反本承诺书而给甲方造成的不利影响，且乙方应自行承担费用按甲方的指示采取有效的方法对保密信息进行保密。

5.1.2 乙方须向甲方支付人民币贰拾万元整（￥200,000 元）的违约金。

5.1.3 如乙方违反本承诺书行为给甲方造成损失，乙方还应赔偿甲方因此遭受的全部损失，在此所称的甲方损失包括但不限于：甲方直接和间接损失、甲方因调查乙方违约并向其主张权利而支出的调查费、误工费、交通费、律师费、诉讼费以及其他因此而支出的全部合理费用。

5.1.4 乙方因违反本承诺书约定，披露保密信息而获得的全部收益，均归甲方所有。

5.2 以上处理并不影响甲方同时根据本承诺书或有关法律采取其他救济措施的权利。

乙方授权代表签字：

乙方盖章

2017 年 12 月 18 日

附件 C：

项目责任书

甲方（国家知识产权局专利局）与乙方（北京中软泰和科技有限公司）于 2017 年 12 月 18 日签订国家知识产权局专利局网络安全运营服务项目 合同，乙方承诺并遵守以下规定。

一、出入规定

1、严格遵守甲方有关人员、物品出入大门、治安、户籍、交通、环保、卫生等有关规定。

2、对要带走的工具、设备，乙方要提前告知甲方，并须由甲方项目负责人协助办理出门条后方可带出。

3、车辆或人员进入甲方区域内，要严格按照规定路线行驶或活动，不得随便进入与本项目无关的办公区域。

二、防火规定

1、必须做好防火工作，要有防火负责人，要建立灭火队伍，要健全防火安全责任制，要配置必要的灭火设施。

2、要明确防火通道，不得随意堵塞，不得压盖地下消防栓，并要有明显标志。

3、动用明火要向甲方防火办申请“用火证”，取得用火证后方可动用明火，必要时还需指派专人进行现场护理。

4、要对电源、电线、用电进行严格管理，严禁随意乱拉临时线，严禁使用电炉取暖。

5、一旦发生火灾要积极抢救，尽快扑灭火灾，并要保护好火灾现场，对弄虚作假破坏现场的，甲方将进行调查，并提请有关部门依法处理。

三、成品保护

1、严格控制进出场的工程物资、设备的搬运，采取铺垫保护性材料等方式保护地面。

2、不得影响其他工作人员的正常工作，要对相关设备做好管理，防止损坏；及时清理施工垃圾，严禁随意抛洒，做到工完料清。

3、经检验后的每道工序采取相应保护措施，保证下一道工序顺利进行。

4、对本项目的工作区域内实行独自管理，发生任何失误、损失、伤亡由乙方自负；若影响到甲方，根据情节轻重追究乙方责任，并由乙方负责相应赔偿。

四、保密规定

乙方要对工作人员进行保密教育，项目相关人员应保守工作秘密，严格控制无关人员进入甲方大楼。项目相关的所有软、硬件信息资料要严格管理，严禁泄密，否则按照有关法律法规进行追究。

乙方签字：

盖章

2017年 12月18日