**采购需求**

**说明：**

1、为落实政府采购政策需满足的要求：

（1）本竞争性磋商文件所称中小企业必须符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定。

（2）服务项目中包含货物的，根据《财政部 发展改革委 生态环境部 市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）和《关于印发节能产品政府采购品目清单的通知》（财库〔2019〕19号）的规定，采购需求中的产品属于节能产品政府采购品目清单内标注“★”的，供应商必须在响应文件中提供所竞标产品有效期内的节能产品认证证书复印件（加盖供应商公章），**否则响应文件按无效处理**。如本项目包含的配套货物属于品目清单内非标注“★”的产品时，应优先采购，具体详见“第四章 评审程序、评审方法和评审标准”。

**2、“实质性要求”是指磋商文件中已经指明不满足响应文件则按无效响应处理的条款，或者不能负偏离的条款，或者采购需求中带“▲”的条款。**

3、如竞标产品存在侵犯他人的知识产权或者专利成果行为的，应承担相应法律责任。

4、供应商必须自行为其竞标产品侵犯他人的知识产权或者专利成果的行为承担相应法律责任。

5、本项目采购标的对应的中小企业划分标准所属行业名称：**软件和信息技术服务业**。中小企业划分标准详见本章附件1。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分标：1** | | | | |
| **需求一览表** | 序号 | 标的名称 | 数量及单位 | 技术要求 |
| 1 | 统计信息化基础设施运维服务 | 1项 | 运维及驻场服务  ▲为采购人的系统平台提供各类信息技术服务，主要包括：  **1、信息化机房运维服务：**  1.1为采购人中心机房的空调系统、动力环境监控系统、七氟丙烷气体消防系统、防雷接地保护系统、配电系统、机房综合布线、视频安防监控系统等机房基础环境提供例行检查及状态监控、响应支持、故障处理、查线打标等服务。  1.2要求提供不少于1年2次的机房清洁服务，包括机房静电地板、设备机柜、机柜设备表面等设施的清洁除尘工作。  1.3提供不少于1年4次的机房空调主机除尘、外机清洗、更换过滤网易耗品件工作。  1.4提供不少于1年4次的UPS不间断电源系统蓄电池的内阻检测，并形成报告。  **2、网络运维服务：**  为采购人办公楼网络、联网直报系统、邮件系统、办公系统等业务系统所涉及的网络设备和安全设备提供网络运维服务，要求如下：  2.1日常维护：网络设备清洁；网络设备运行状态巡查；线路连接状态巡查；设备标签制作、粘贴检查；线路整理；设备日志记录检查；日常维护工作日志生成并提交。  2.2故障处理：故障的排除、恢复；确认排除、恢复的结果；提交故障处理报告。  2.3实时监控：线路连接状态监控；设备供电状态监控；设备状态灯监控；设备风扇状态监控；网络丢包率；CPU使用率；内存使用率；网络连通性监控；网络延时监控；监控报告；网络设备端口/链路流量监控；网络链路错误率测试等。  2.4定期巡检：系统可用性检查；系统性能检查；提交巡检报告。  2.5性能优化：定期评估网络运行状况，软件版本、特征库等升级并及时更新网络安全策略，对网络健壮性、安全性、负载冗余等内容做网络链路状况、设备负荷、传输质量等专业分析，提供全面、合理的网络架构优化方案。  **3、主机运维服务：**  为采购人管理的主机设备（包括服务器、存储及小型机）提供以下运维服务。  3.1定期对主机设备性能进行监控，对于主机设备性能存在异常或超出阈值的，应及时记录并反馈。  3.2根据管理需求，对主机设备进行添加、修改及删除等操作，并及时操作记录形成纸质或留痕。  3.3日常维护：CPU、内存扩容升级、RAID重建、更换损坏备件等；微码升级服务；主机设备清洁；标签制作、粘贴；线路整理；磁盘检查；逻辑卷空间调整；设备日志检查；周期性日志清理；日常维护工作日志生成并提交。  3.4设备巡检：系统可用性检查；系统性能检查；提交巡检报告。  3.5故障处理：故障的排查、分析；故障的排除、恢复；确认排除、恢复的结果；提交故障处理报告。  3.6日常监测：设备状态灯检查；设备连接线检查；设备电源状态检查；设备风扇状态检查；设备硬件检测；服务器CPU使用率；服务器内存使用率；文件系统使用率；交换区使用率；服务器连通性状况检测。存储设备状态灯检查；存储设备连通状态检查；存储阵列状态；硬盘物理状态；硬盘逻辑状态；热备盘接管状态；存储CACHE状态；磁盘适配卡状态；磁盘通道状态；主机通道卡状态；主机通道状态；电源模块状态。  3.7性能优化：分析性能瓶颈；优化措施制定；优化措施执行。  3.8服务器、存储等设备硬件维保服务：为采购人主机设备（设备清单详见本分标附表1）提供运维期间的硬件维保服务，必要时提供备件以保证系统的正常运行。  3.9网络存储设备版本升级服务：为采购人网络存储设备进行版本升级，升级时需确保数据安全**。**  **4、桌面终端运维服务：**  4.1区局办公楼办公终端及外设（台式机、便携式计算机、一体机、打印机、复印机、投影机、扫描仪、传真机等）的使用支持、故障排除、操作系统安装配置调试等。  4.2日常办公软件维护（WPS、PDF等基础支撑软件）。  4.3终端安全软件维护：及时处理终端设备的木马病毒防护、补丁工作。  **5、视频会议系统运维服务：**  5.1视频会议包括国家统计局和区局召开的涉及全区统计系统的会议，负责区局视频会议系统的操作和保障，提供会议前准备工作，包含区局会场扩声系统调试、视频会议系统联调、网络优化服务，会议召开期间提供经过现系统认证的视频会议工程师进行驻场会议保障服务，确保相关设备稳定运行、会议正常召开。  5.2负责区局7楼大会议室及多功能厅视频会议系统中涉及的子系统主要包含会议环境系统、显示系统、扩声系统、会议发言系统、指挥坐席系统、会议管理系统、综合布线系统的维护。  **6、超融合、存储设备系统升级服务：**  服务期内对所列超融合、存储设备从脱保之日起至2026年12月31日提供维保升级服务。  6.1超融合计算节点系统升级  服务要求：提供深信服超融合计算节点软件升级服务，服务期限为合同签订之日起1年：设备型号为：深信服超融合计算节点aServer-2300，数量：16台，设备于2025年5月30日过保。升级后要求支持具备内存纠错保障业务连续稳定运行、集群动态资源调度功能、定时自动备份和立即备份两种备份方式，可设置备份策略、补丁机制支持升级与回滚等功能。在响应文件中提供软件升级方案，升级后原有系统服务内容说明文件，包含服务期内软件升级条款、服务响应机制、售后服务机构的设置及售后工程师名单、联系方式。  6.2存储设备系统升级  服务要求：对以下存储设备购买原厂升级服务，设备软件在服务期内升级到最新稳定版本，包含硬件保修服务。设备清单：1台备份一体机爱数VX2400，2台华为CE6881-48S6CQ-B交换机，2台华为OceanStor 5300 v5及扩展柜，2台华为DPA3610，1台爱数E6020。  **7、IT运维可视化服务：**  服务要求：提供一套IT运维可视化软件，使用许可期限为合同签订之日起1年，部署方式：本地部署，用于提高运维效率,提升服务质量,降低运维成本,改变孤立、分散的IT管理。功能要求如下：  7.1平台采用B/S架构，支持在发行版Linux和国产信创操作系统等不同平台下部署，采用模块化开发，支持分布式部署。  7.2可管理IT资产数（IP）：500；支持资产包括网络设备、安全设备、存储设备、虚拟化平台及机房动环系统等，并提供灵活的自定义方式，具备多种类型的动态效果，可自定义视图。  7.3支持大屏展示、告警模块、拓扑管理、主机管理、模板管理、报表管理、用户管理、配置管理等运维管理模块。  7.4支持配置拓扑图，并对拓扑图中的告警设备进行实时的轮询动态播放。  7.5支持定制模板，可基于ICMP、SNMP、SQL、JMX、IPMI、TELNET、SSH等方式进行定义，支持指标以自定义方式展示到相应的资源，支持折线、表格、仪表盘等多种展示方式；  7.6支持对操作系统监控，包括Windows 2012/2016/2019的32位/64位（中英文各版本）、Linux等操作系统，支持对CPU利用率、内存利用率、磁盘利用率、网卡状态、进程等信息的采集，支持自定义脚本采集。  7.7支持对数据库监控，包含MySQL、oracle、SqlServer、redis、mongdb等数据库的监控，支持对数据库状态、连接数、表空间、表空间使用率、服务进程等信息的采集，支持自定义脚本采集。  7.8支持对Tomcat、weblogic、websphere、jboss等中间件的监测，包括连接响应时间、servlet运行池情况、节点状态、内存空间和使用率、线程数、传输字节速率等信息的采集，支持自定义脚本采集。  7.9支持对WEB应用进行状态监控。  **8、业务系统渗透测试服务：**  服务内容：提供一次二级站点业务系统的渗透测试服务，通过情报搜集工作，进行威胁建模和攻击规划，以主流渗透工具模拟黑客攻击为主要手段，发现常见的高中危漏洞为主要目标，将发现的安全漏洞进行整理，给出详细说明，并针对安全漏洞逐一提供的解决方法。渗透测试工作全部完成后输出《业务系统渗透测试报告》，报告中阐明客户系统中存在的安全隐患以及专业的漏洞风险处置建议。  **9、为采购人提供指定的信息技术咨询：**  对采购人服务器、网络设备、网络安全部署现状提出合理化建议。采购人发生网络调整改造、硬件安装升级时，协助采购人进行网络规划及配置，以及相关技术培训服务。  **10、重大活动期间（如两会、中国--东盟博览会等）提供重点保障服务:**  重大节假日期间（重大节假日：如元旦、春节、端午节、中秋节、国庆节等国家/自治区法定节假日）提供轮值保障服务，同时按要求提供现场值班服务。  **11、运维人员要求：**  在合同约定的维护期内提供至少一名具有3年相关IT运维工作经验的驻场工程师。驻场工程师上班时间与采购人同步，每天按采购人上班时间进行考核。成交供应商运维人员在服务期间，必须遵守采购人制定的各项关于机房设备及业务系统运维的管理制度。  **12、故障处理响应要求：**  故障电话响应（365天×24小时/天）；故障现场服务（7天/周×24小时/天）；发生故障时，驻场工程师如无法排查恢复，成交供应商的运维保障支持团队人员在1小时内到达现场并进行故障恢复。  **13、运维文档管理：**  13.1按采购人相关制度要求，运维服务过程中定期备份必要的记录和日志文件，这些文件包括但不限于信息资产清单表、网络拓扑图、机房日常巡检记录表、驻场运维工作日报、月度运维服务报告、季度运维服务报告、年度运维服务报告、故障处理登记表、机房设备登记表、安全检查总结报告。  13.2合同期满前两周，驻场运维工程师须全面整理整个服务项目内完成的各项文档、数据，进行必要的资源移交工作准备。 |
| **商务条款** | **规范标准：**  采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。  **服务期限及地点：**  1、服务期限：自签订合同之日起1年。  2、服务地点：广西南宁市内采购人指定地点。  **付款条件：**  在合同签订后10个工作日内，成交供应商向采购人提交初步运维方案。采购人确认运维方案后，向成交供应商支付合同价款的70%。余款由采购人视工作开展、验收情况及预算执行情况支付（验收工作如需外聘专家，专家评审费由成交供应商承担）。  **其他要求：**  一、总体要求  1、响应文件中可提供针对本项目的运维服务方案、服务能力保障方案、服务技术能力材料、信誉及业绩材料。  二、验收要求及标准  1、根据采购需求的要求进行验收。  三、其它  1、供应商须具备独立完成项目，不得以任何形式转包；  2、供应商可在响应文件中对采购需求做出响应。一旦成交之后须严格按照采购要求及响应承诺提供服务，确保系统的正常运行。在维护过程中必须承担数据丢失、设备损坏等方面的风险，若由于成交供应商自身技术不足或违规操作等原因造成的数据丢失、设备损坏等，须承担相应的责任。  3、要求具备及时的故障响应及处理机制，针对运维系统制定相应的咨询和培训服务计划，提供相应的咨询和培训服务。  4、成交供应商及提供技术服务的工程师需与采购人签订保密协议，不得泄露采购人组织及系统信息。  5、供应商拟投入的技术服务人员须为供应商的在职员工，成交后，成交供应商须向采购人提交技术服务人员的基本信息及成交供应商为其缴纳近一年内任意连续1个月的社保证明材料、资质证书复印件等，无法提供材料或提供的材料中人员信息与响应文件不符的，采购人有权不予签订合同并上报监督部门依法追究其责任。 | | | |

**分标1 附表1**

**设备清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 品牌型号 | 数量 | 备 注 |
| 1 | 服务器 | 浪潮英信NF8480M4 | 13 |  |
| 2 | 服务器 | 浪潮天梭TS860G3 | 1 |  |
| 3 | 服务器 | 浪潮英信NF5280M4 | 2 |  |
| 4 | 超融合计算节点 | 深信服超融合计算节点aServer-2300 | 16 |  |
| 5 | 服务器 | 华为RH5885v3 | 3 |  |
| 6 | 服务器 | 华为RH2288v3 | 5 |  |
| 7 | 服务器 | 曙光SugonI980-G20 | 1 |  |
| 8 | 服务器 | 华为RH2488H v5 | 2 |  |
| 9 | 备份一体机 | 爱数VX2400 | 1 |  |
| 10 | 存储 | 浪潮AS8000-M2 | 2 |  |
| 11 | 万兆交换机 | 华为CE6881-48S6CQ-B交换机 | 2 |  |
| 12 | 存储 | 华为OceanStor 5300 v5 | 2 |  |
| 13 | 存储扩展柜 | 华为硬盘框 | 2 |  |
| 14 | 100T备份一体机 | 华为DPA3610 | 2 |  |
| 15 | 备份一体机 | 爱数连续业务应急保护设备E6020 | 1 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分标：2** | | | | |
| **需求一览表** | 序号 | 标的名称 | 数量及单位 | 技术要求 |
| 1 | 数据中心机房网络安全软件和硬件设备续保及应急演练服务 | 1项 | **一、服务涉及对象产品清单列表如下(设备清单仅供参考，具体以采购人现场安装设备为准)**  ▲（一）安全设备产品类：  1、深信服防火墙 AF-1820-F5 3台 ；  2、深信服防火墙 AF-1800-D1 8台；  3、深信服VPN VPN-4050-D1 1台；  4、深信服威胁探针 STA-100-B440 1台  5、深信服态势感知 SIP-1000-B400 1台；  6、深信服上网行为管理系统 AC-H6500 1台；  7、深信服终端安全管理系统：提供1年软件授权（包含：Windows终端安装授权200点、Windows服务器安装授权100点、Linux服务器安装授权50点）；  8、深信服国产化终端安全管理系统：提供1年软件授权（包含：终端安装授权270点）  9、迪普IPS2000-GS-E 4台；  10、深信服NIPS-2000-B2100 1台；  10、科来网络回溯分析平台 1台；  11、深信服防火墙 AF-2000-B2150，3台；  12、深信服堡垒机 OSM-1000-B2100 2台；  13、深信服数据库审计系统 DAS-1000-A640S 1台；  14、深信服云镜 YJ-1000-B1075 1台；  15、深信服全网行为管理系统 AC-1000-B1300-ID 1台；  16、深信服零信任访问控制系统 aTrust-B1050M 1台；  17、深信服态势感知平台第三方接入授权软件（含第三方设备10个接入授权）。  ▲（二）安全服务类：  18、钓鱼邮件演练服务：结合采购人网络环境、邮件使用习惯和特征，以热点事件为主题，精心构造极具迷惑性且含有恶意链接、恶意附件的邮件，向目标群体定向开展邮件钓鱼测试，并根据演练结果为采购人提供安全培训和技术防护手段升级建议。  19、应急演练服务：针对我局目前现有防御措施（包括可能的实时动态防御）进行评估渗透，对目标系统、人员、软硬件设备、基础架构，进行多维度、多手段、对抗性模拟攻击，并提供攻防实战演练报告，攻防演练时期分为三个阶段，即备战阶段、实战阶段和总结阶段，包含云端及本地两种服务方案，涵盖从资产梳理、脆弱性识别、安全加固、攻防演练等方面，最终帮助采购人实现纵深网络安全防御，建立持续有效的网络安全运营机制。  20、配合采购人，完成统计业务专网向电子政务外网迁移整合工作。  **二、服务具体服务质量及要求**  ▲（一）服务期内对所列设备从脱保之日起至2026年12月31日提供维保升级服务。  （二）对采购人本次采购的服务对象（见上对象清单列表）提供日常检查监控、定期维保，提供有关技术支持服务等，保证服务对象安全稳定持续运行。  ▲（三）要求每月完成一次全系统巡检工作。巡检内容包括系统硬件、软件运行情况，并根据运行情况提交系统详细报告，对系统存在的缺陷以及各类即将发生的故障有提前预判方案以及预防措施，对非硬件突发的故障能够提前做好各类挽救措施以及准备预防工作，发现异常状况，必须在2小时内予以解决。  ▲（四）每季度定期对维保设备包括所有安全设备产品进行系统备份，在系统有所改动、升级、安装新应用前、后都须做好系统备份。  ▲（五）对故障部件等主体故障部件，提供优于市场价的备件支持。  ▲（六）安全设备产品服务内容具体服务要求：  **1、安全设备产品维护服务要求：**  （1）提供设备硬件的现场升级服务；  （2）提供系统软、硬件故障诊断、性能调整、参数优化及现场维护服务；  （3）协助用户制订日常维护方案，如系统备份及恢复方案等；  （4）每次现场服务结束后，为用户提供详细的技术文档；  （5）每月对设备及系统进行巡检、出具月度运行报告；  （6）提供日常检查监控、定期维保、备品备件、坏件的及时更换、修复等；  （7）根据用户要求，配合优化网络配置，加入防火墙、VPN、态势感知等安全设备的策略，确保机房能信息安全要求。 |
| **商务条款** | **规范标准：**  采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。  **服务期限及地点：**  服务期限：服务期1年。  **服务地点：**  广西南宁市内采购人指定地点。  **售后服务要求：**  接到服务请求后，故障电话半小时内响应，2小时内到达现场，紧急时刻1小时内到达现场提供技术支持；在不需要更换备件的条件下在12小时内解除故障。硬件故障需要更换的，24小时内提供相同性能参数的备件替用；配件需要返厂维修的，在2日内完成相关厂家配件更换及硬件修复，解决故障。故障解决后，向采购人提交故障处理报告。  **付款方式：**  在合同签订后10个工作日内，成交供应商向采购人提交初步工作方案。采购人确认工作方案后，向成交供应商支付合同价款的70%。余款由采购人视工作开展、验收情况及预算执行情况支付（验收工作如需外聘专家，专家评审费由成交供应商承担）。  **其他要求：**  1、报价应包括网络与硬件维护、耗材及服务的费用，包括采购、运输、劳务、管理、利润、税金、保险、协调、售后服务、配送以及所有不确定因素的风险等可能发生的一切费用。对于本文件中未列明，而供应商认为必需的费用也需列入总报价。在合同实施时，采购人将不予支付成交供应商没有列入的项目费用，并认为此项目的费用已包括在总报价中。  2、供应商须为本项目服务实施投入充足的服务人员，并确保响应文件中的人员信息真实、有效。  3、供应商拟投入的技术服务人员须为供应商的在职员工，成交后，成交供应商须向采购人提交技术服务人员的基本信息及成交供应商为其缴纳近一年内任意连续1个月的社保证明材料、资质证书复印件等，无法提供材料或提供的材料中人员信息与响应文件不符的，采购人有权不予签订合同并上报监督部门依法追究其责任。  4、未经采购人允许，不得使用或以其它方式给任何第三方提供本项目的相关信息或数据。  5、成交供应商不得将项目非法分包或转包给任何单位和个人，否则采购人有权即刻终止合同，并要求成交供应商赔偿相应损失。  6、知识产权：采购人在中华人民共和国境内使用成交供应商提供的产品及服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉。如果第三方提出侵权指控，成交供应商应承担由此而引起的一切法律责任和费用。  7、供应商可按照采购需求在响应文件中提供详细、科学、可行的运维服务方案、售后服务（可包含投入人员安排、进度计划安排等内容）。  8、供应商如有可在响应文件中提供服务承诺以及与本项目相关的信誉、业绩、奖项等证明材料。  9、为了保障服务能力及使用效果，本项目响应文件中信息化设备、系统运行维护服务如有设备同品牌原厂授权书，如有可提供供磋商小组评审参考。  10、验收要求及标准：根据采购需求的要求进行验收。 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分标：3** | | | | |
| **需求一览表** | 序号 | 标的名称 | 数量及单位 | 技术要求 |
| 1 | 网络安全运维及“重保”服务 | 1项 | ▲1、人员要求  提供2人次1年5×8小时（12个月）的驻场服务，要求全日制本科及以上计算机相关专业学历，其中一人需具备4年及以上驻场运维工作经验，另一人需具备1年及以上驻场运维工作经验，入场服务时需提供学历证明，拟投入现场驻场人员须经过采购人面试同意后确定。对IT资产梳理与漏洞管理、安全设备日常运维、安全事件分析研判、加固整改、应急事件处置、重保期间安全保障等工作。  ▲2、设备巡检  对所有安全设备每天运行状态巡检和检测，及时发现并消除日常运行过程中的安全隐患，确保设备正常运行。日志分析、故障诊断与故障预警、性能评估等工作，对安全设备的运行情况进行梳理、检查、全面测试和分析。确认设备运行状态，检查设备的日志记录情况，排除故障隐患工作，保证网络及软、硬件设备系统安全、稳定的运行。  提供材料：包括但不限于《安全设备巡检记录表》《设备故障处理报告》《安全设备升级记录表》。  3、安全策略优化梳理服务  定期对采购人防火墙安全策略配置进行优化和清理，对策略变更进行记录，发现过期、冗余、无效、不明确用途等策略，根据分析结果提供优化调整建议。  提供材料：包括但不限于《策略记录更新表》《防火墙策略优化报告》。  ▲ 4、数据安全风险评估服务  对采购人1个应用系统进行2次数据安全风险评估。  评估依据《GB/T 45577-2025数据安全技术 数据安全风险评估方法》《统计数据安全管理办法》《统计数据分类分级标准规范》等标准进行，主要包括五大部分。最终出具评估报告（包括初评和复评）。  评估准备，是数据安全风险评估的初始预备阶段，在评估实施前应完成评估准备工作。形成调研表、数据安全风险评估方案等。  信息调研，主要用于识别数据处理者的基本情况，厘清其与业务和信息系统的关系，处理的数据和开展的数据处理活动情况，采取的数据安全防护措施。形成数据处理者基本情况、业务清单、信息系统清单、数据资产清单、数据处理活动清单、安全措施情况等，具备条件的，可绘制数据流图。  风险识别，针对评估对象，从数据安全管理、数据处理活动、数据安全技术、个人信息保护等方面，通过多种评估手段识别可能存在的数据安全风险隐患。形成文档查阅记录文档、人员访谈记录文档、安全核查记录文档、技术检测报告等。  风险分析与评价，在风险识别基础上开展风险分析，并视情对风险进行评价，最后提出整改建议。形成数据安全风险源清单、数据安全风险列表、整改建议等。  评估总结，编制数据安全风险评估报告，开展风险处置。  5、资产与漏洞管理服务  **资产管理**：具有资产发现，端口探测的能力，能够具有对主机的存活状态、端口等基础信息识别；对资产状态检测、收集、识别资产上线、下线和更新状态；能够对子域名发现，具备对主机、网站、域名三种类型资产管理能力。各类资产包括：安全设备、存储设备、服务器、数据库及中间件、业务资产等。  定期盘点机房资产并形成资产台账，梳理易受攻击的应用系统目标（重点资产），协助对资产存活状态、访问行为进行动态管理，配合完成对资产密码的梳理及改密服务。  **提供材料**：提供并定期更新《资产信息及状态表》。  **漏洞管理**：能够检测常见的操作系统漏洞、软件漏洞、最新的网站框架应用漏洞，弱口令检测，网站WEB漏洞等。基线检测、对禁止端口及服务开放基线设定确认是否已开放。提供修复整改意见并协助整改。整改完成还要进行漏洞复测，对整改效果进行检测，形成漏洞管理闭环。  针对最新公开漏洞（如CVE、CNNVD等）以及国家统计局或者网信部分发布的漏洞通知，分析对自治区局系统的影响情况，进行相应漏洞修复、提出规避建议。  提供材料：包括但不限于《漏洞检测报告》《漏洞处理及复测记录》等。  6、数据安全设备分析  每日对采购人网络中数据安全类设备进行安全巡检和安全情况进行初步评估分析，包括设备硬件状态巡检、性能巡检、数据安全设备告警日志基础分析研判，并结合网络安全设备形成联合分析能力，快速定位受害目标和攻击源。  提供材料：包括但不限于《安全设备巡检记录表》《数据安全分析报告》等。  7、全流量回溯分析服务  （1）使用采购人现有科来的网络回溯分析系统通过监控网络全流量，展现网络关键节点真实的通信状况，掌握全网运行状态，洞悉关键业务应用状况，针对网络/应用总体质量、网络/应用性能、网络/应用安全等方面全面评估分析，对网络异常通讯行为进行数据包分析，发现异常的流量、异常的网络行为、蠕虫病毒、木马和网络攻击等，对攻击事件溯源取证，直接定位问题根源，保障关键业务畅通。  网络总体质量评估  对现有业务数据进行L2至L7层的协议识别和解析数据包具有分析能力，提供网络各层的性能指标和评估结果，并根据各项指标评估结果得出现有网络的整体健康安全趋势，如果当前网络存在性能或安全问题需要在分析报告中进行明确体现。  （2）网络运行质量评估分析  为提升采购人日常网络运维效率，掌握实时网络运行质量，为运维提供数据依据，要求提供实时1秒级网络运行质量评估分析服务，基于网络流量指标关键KPI进行实时统计分析，生成图形化的报表，评估网络运行质量。要求网络运行质量评估分析的指标项包含如下：  能够反映实时流量的趋势变化，要做到包括总体流量的趋势，数据包趋势， TCP参数趋势，利用率趋势。  统计任意时间范围内网络应用的成分占比及流量信息，包括接收发送流量，接收发送数据包等。  统计任意时间范围内所有IP主机的通讯流量信息，统计指标项至少包括接收发送流量，接收发送数据包，比特率，数据包率，tcp连接请求数量，tcp同步响应数量，tcp同步重置数量，数据包的发收比，tcp连接请求无响应次数，tcp连接请求被重置次数等流量参数。  服务器安全性评估分析，统计网络中关键服务器提供的服务端口，并核对是否存在非法端口被访问。  （3）网络数据包深度分析  网络故障日益复杂，而数据最终是以数据包进行传输，因此要剖析故障的根本原因就离不开数据包深度分析，要求能够针对数据包提供L2-L7层解码分析，通过数据包深度解码分析快速定位故障的层级，数据包深度分析服务内容要求如下：  统计分析任意指定对象（如:TCP/UDP会话五元组、服务节点开放的TCP/UDP的服务端口、客户端到服务器服务端口的全量访问统计）的1秒级精度流量，包率等曲线，并根据用户所选时间展示精度1秒的全量关联分析统计数据。  为了更快速高效的定位网络故障，服务要实现对故障智能诊断的能力，能自动诊断包括：HTTP错误、SMTP/POP3服务器慢响应、SMTP/POP3服务器返回错误、FTP服务器慢响应、FTP服务器错误、TCP连接被拒绝、TCP非法校验和、TCP重复的连接尝试、DNS错误、会话连接故障、重传、IP TTL太小、IP地址冲突等常见故障场景，并提供故障原因分析及解决办法。  （4）应用运行质量评估分析  当应用系统访问质量出现异常时，分析服务要能根据通过丰富的KPI性能指标评估系统运行质量的好坏，及时发现应用系统性能故障，要求提供的服务报告中体现的KPI指标至少包括：TCP连接请求无响应次数、TCP连接请求被重置次数、RTT、TCP ACK时延、重传数量、重传率、分段丢失率、会话数量（新建会话数量，关闭会话数量，活动会话数量）、TCP 0窗口数量、交易处理数量、响应时间（平均响应时间，最大响应时间，最小响应时间）等。  （5）异常安全威胁评估分析服务  能提供安全威胁分析检测服务，并能够针对异常威胁流量及时反映给运维人员，方式不限于人为通报和服务设备自动告警。服务内容要求如下：  至少能够提供针对网络中的ARP攻击，拒绝服务攻击，DOS攻击，TCP端口扫描，HTTP、SMTP、POP3可疑会话行为的分析。  能够对各种KPI指标的多种参数逻辑或、逻辑与的灵活组合通报，通报事件至少包括1秒、10秒、1分钟等精度。  可人为分析或分析设备自动告警发现木马、病毒事件，支持基于自定义木马病毒特征值、可疑域名、邮件敏感特征值的流量监测，监测异常的TCP/UDP通讯并产生告警，以便准确掌握安全异常的问题主机。  支持基于异常访问的黑白名单访问实时通报。通过设定主机、应用的黑名单，发现异常网络访问并实时通报给运维人员。  ▲（6）服务要求：每月及重大活动时期提供《网络异常流量回溯分析报告》，每年不少于12次；  为保障采购人网络内重大疑难异常问题准确、高效的解决，供应商须在响应文件中提供具备现有科来网络回溯分析系统制造商专家技术支持的服务能力承诺函（格式自拟，加盖供应商公章）。  ▲8、网络异常回溯备机服务  为了保证采购人对全网异常流量采集的全面性，供应商须提供功能一致并与现有系统稳定对接的备用设备，备机须在服务期内放置采购人机房使用。  在首次递交的响应文件中提供此项服务承诺函扫描件（格式自拟）。  （注：成交签订合同后，成交供应商须提供网络回溯分析系统备用设备1台，功能需与现有网络中使用网络回溯分析系统功能一致，采购人有权测试验证，如在测试中发现两者功能不相符及授权未注明采购人信息，采购人将不予验收，并追究其相关责任。）  ▲9、业务运行安全监控服务  为达到以业务为核心的监控视图，将采购人现有的业务性能管理系统、科来网络回溯分析系统与供应商提供的网络异常回溯备机兼容配套使用，采集分析回溯分析系统的应用性能指标参数和应用报警信息，包括但不限于链路流量、应用、业务、会话等多维度的各类参数信息，同时业务性能管理系统能够将应用、警报和网段配置信息下发给网络回溯分析系统及网络异常回溯备机，实现采购人应用系统应用服务、主机系统、网络路径梳理和监控分析策略和警报策略下发。  业务性能管理系统、网络回溯分析系统及网络异常回溯备机需实现业务访问路径梳理、分级及告警策略下发等工作，要求在签订合同后五个工作日内完成。  在首次递交的响应文件中提供以上此项服务的响应承诺函扫描件（格式自拟）。  10、安全运营服务  为了保障采购人网络与业务系统安全平稳运行，需根据已有的网络安全设备及新增安全服务相结合，从防御、检测、响应、预测四个维度，以持续监控和分析为核心提供安全服务。  防御层面：对IT资产漏洞、风险暴露面全面扫描探测；防火墙、WAF、抗DDOS等安全防护设备策略优化设置。  检测层面：对威胁感知系统、回溯分析系统、入侵检测等检测设备告警事件进行综合日志关联分析、研判，提升检测效率、达到降低威胁停留时间及损害。  响应层面：协助采购人及时修复IT资产漏洞、对安全策略配置定期优化，收紧威胁暴露面。通过对应用系统的访问日志、网络安全设备日志等日志信息，操作系统、安全设备产生的告警事件，结合网络回溯分析系统和开源的威胁情报信息，综合找出存留的攻击者痕迹，发现并回溯曾经发生的安全事件，从而确认系统是否已被黑客成功入侵、应用系统安全事件入侵路径、遭受利用的安全漏洞信息及造成的安全损失与影响范围。  预测层面：内部利用安全设备策略优化、制定访问基线；外部利用新一代威胁感知系统威胁情报攻击事件预测；形成内外结合攻击预判，同时将预判结果利用到防御、检测、响应环节形成安全闭环。  提供材料：《安全运营季度服务报告》《安全策略变更记录表》；《安全运营季度服务报告》报告内容至少包括漏洞及风险暴露面检查、整改情况、安全设备策略配置情况、风险收敛及策略优化实施情况、安全事件统计及分析、问题总结及优化建议等。  ▲11、安全监测细化分析及处置  驻场人员需对采购人所有安全系统及设备的事件进行分析，梳理某一段时间的信息安全情势、安全状况，提出改进建议，总结、提炼态势研判报告。对全区的安全态势、恶意软件使用情况、网页漏洞利用情况、APT事件、服务器类失陷事件和漏洞利用成功事件进行影响分析。  驻场人员需具备态势感知、IPS、蜜罐及防火墙与网络回溯分析系统告警信息形成联动分析及处置的能力，能分析识别每个安全设备告警的事件（威胁）的来源、影响和重要性，及时发现潜藏在网络中的安全威胁；若出现严重安全事件时供应商需组织专业安全服务人员与驻场人员形成团队协作进行分析研判，实现对恶意行为实现快速发现，对采购人受害目标及攻击源头进行精准定位，对入侵途径及攻击者进行的研判与溯源，从源头上解决采购人网络中的安全问题，并最终形成详细的分析研判报告，定期报告给采购人。  具备同步分享上级主管部门网络安全事件监测分析、研判处置等方面经验，能够排查、整改上级主管部门和网络安全相关部门发布的网络风险问题，以提高采购人网络安全事件综合应对能力。  供应商须在首次递交的响应文件中提供此项内容的承诺函扫描件（格式自拟）。  （注：成交签订合同后，成交供应商须提供具有同步分享上级主管部门安全处置经验能力的证明材料，若不提供采购人不予验收，并追究其相关责任。）  提供材料：定期提供《安全监测联动分析报告》，每年不少于12次；根据工作实际按需提供网络安全风险情况排查整改的情况汇总表或报告。  12、安全咨询服务  需对采购人的网络安全工作提供咨询服务，配合采购人围绕上级网络安全主管部门的要求，对网络安全工作部署、安全检查、年度安全考核等工作进行详细规划。  13、日常技术保障服务  对采购人全区14个地市局安全监测工作，对收集各地市态势感知产生的安全告警事件分析研判，并协助自治区局对各地市安全事件通报，对全区的安全态势、恶意软件使用情况、网页漏洞利用情况、APT事件、服务器类失陷事件和漏洞利用成功事件进行影响分析；出现突发、紧急安全事件时，协助区局做好应急支持工作，大限度地减少信息系统的损失和负面影响。  以安全专报的形式对区统计局及所辖各市、县（市、区）定期进行网络及数据安全情况通报，内容包括：安全通报文件、漏洞详情、整改建议、其他应当知晓的情况。  安全问题协助整改，配合自治区局人员根据需要到地市现场进行指导安全问题整改，安全防护墙等设备策略定期检查工作，指导各风险收敛和定期对防火墙策略配置优化、梳理。  14、重要时期安全保障服务  （1）需在两会、攻防演习等重大活动期间提供保障服务。在安全运营服务工作基础上，一方面加强网络访问控制、应用系统评估与加固等服务；  资产梳理：有针对性梳理现有重要系统的网络路径、网络拓扑和相关资产信息，整理并确定网络安全专项应急预案。  风险消除：进行安全自查和整改，对现有主机进行安全自查和安全加固，基础安全自查（包括但不限于配置核查、漏洞扫描、安全机制校验），业务风险分析（包括但不限于潜在风险梳理、风险对抗手法），能够通过安全自查发现的问题，进行整改、加固和完善。  立体防御：利用现有的监测与分析设备，实时采集网络流量、日志、可疑事件相关信息，确保能够持续对网络攻击进行实时监测，并及时进行响应处置，针对监测中发现的漏洞和弱点，及时进行修补和加固，积极应对，协同进行安全处置。  溯源分析：通过现有设备日志等信息对攻击行为进行分析，以找到攻击者的源IP地址、攻击服务器IP地址、邮件地址等信息，并对攻击方法、攻击方式、攻击路径和工具等进行分析研判。  重保后需全面总结防守工作情况，对存在的网络事件从发生到处置结束应有完整的闭环处理流程并作记录。对于期间发现的问题和短板及时进行归纳整改和弥补，总结有效的应对措施和协同处置的规范流程。  提供材料：包括但不限于重保前《安全检查和加固报告》、重保期间《安全事件分析溯源及处置报告》、重保后《重保防守总结报告》。  ▲（2）服务应具备攻击诱捕服务能力，达到混淆攻击者目标，结合采购人在用攻击诱捕工具建立立体安全防护体系，能够溯源分析研判是真人、扫描工具等攻击者，并在攻击者尝试攻击时，进行信息搜集延缓攻击进程，让攻击者不触碰到真实资产，主动暴露攻击者身份、攻击手法、攻击目的等，从而实现攻击隔离。一旦发现真实攻击，立即切断，防止黑客攻击真实业务。攻击诱捕工具须在服务期内放置采购人机房使用。  ▲（3）服务应支持将上级主管部门的蜜网系统诱捕策略、行业情报、溯源信息等内容同步至本项目采购人，构建本采购人与上级主管部门的欺骗防御体系，做到及时全面刻画有关攻击者的攻击行为，可高度感知内网上下级的渗透活动、病毒扩散等高危事件，争取应急响应和攻击取证的时间。供应商须提供有关此项服务的承诺函（承诺函格式自拟，供应商须承诺签订合同后十个工作日内实现上下级有关本项要求的信息内容共享，若不能按时完成的，采购人不予验收，并追究其相关责任。）  攻击诱捕工具技术需求详见本分标附件1。  15、安全通报  根据采购人要求对采购人单位及所辖各市、县（市、区）系统单位定期进行网络信息安全情况通报，内容包括：安全通报文件、漏洞详情、整改建议、其他应当知晓的情况。  安全通告服务频率：根据采购人工作需要确定。  16、应急处置服务  在出现突发、紧急安全事件时，提供7×24小时的应急响应服务，协助采购人有效的应急处理，最大限度地减少信息系统的损失和负面影响。成交供应商应具备完备的应急体系，应急响应服务应满足1小时到达用户现场，4小时恢复系统运行的服务响应指标。  提供材料：应急服务完成后提供《应急响应报告》。  ▲17、恶意代码快速响应服务  为全面提升采购人针对网内已知未知的恶意代码快速反应处置能力，保障应用系统运行安全，供应商需提供1套恶意代码快速检测系统。  系统需支持x86架构及各类国产化架构，满足在常规的Windows、Linux及各类国产化操作系统（包括银河麒麟、深度、统信、凝思、中科方德等）中运行。同时需具备使用灵活，无需部署客户端就能进行检测，做到快速检测、阻断处置的能力，对各类终端起到恶意代码防护作用，成交供应商须在签订合同后提供服务前提供恶意代码检测系统设备商针对本项目恶意样本快速分析及应急响应服务承诺函。  18、安全内容服务  定期提供与采购人工作相关的网络安全材料。提供的材料包括但不限于以下内容，具体根据采购人要求准备：  （1）网络安全方面：及时更新网络拓扑图；提供每季度中某一月的抗拒绝服务系统、应用防火墙、堡垒主机和入侵检测或入侵防御系统安全分析和处置报告；汇总采购人单位及所辖各市、县（市、区）系统单位网络接入情况、出入口情况、网络边界安全防护系统、安全审计系统等情况；每个网络边界的访问控制等安全措施的详细说明文档（含安全系统名称、用途、部署位置、厂商名称和型号，及安全系统的策略截图）  （2）主机安全方面：及时更新服务器及终端台账，包括信创终端和window终端，并统计信创终端和window终端杀毒软件安装比率、感染恶意程序情况等。  （3）应用安全方面：按季度提供信息系统WEB应用层面、数据库层面、主机服务器层面等安全漏洞检测报告及分析情况以及安全整改工作情况；  （4）安全管理方面：协助采购人完善安全管理规章制度，配合完成相关制度落实情况；协助采购人完善网络安全应急预案，提供考核年度内的应急演练实施报告及处置情况记录。  （5）安全监控和审计方面：提供网络安全监控审计情况说明文档（含监控系统、监控对象、监控内容、处置流程等），包括机房环境、网络异常、上网行为、主机、应用系统（直报系统、对外网站、邮件等）、数据库、信息内容、安全运行维护等方面监控情况；提供每季度中某一月的网络安全审计报告（网络审计、主机审计、数据库审计、上网行为审计、安全运维审计等3项及以上），并分析异常情况。 |
| **商务条款** | **规范标准：**  采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。  **服务时间及地点：**  1、服务时间：自签订合同之日起1年。  2、服务地点：广西区内（采购人指定地点）。  **售后服务要求：**  1、免费维护至少1年（自交货并验收合格之日起计）；  2、为保证采购人深信服态势感知系统、科来网络回溯分析系统、数腾业务连续保护系统等核心设备的功能得以充分发挥，设备价值利用率进一步提高，供应商在成交签订合同后，提供上述厂商针对本项目出具的《专项服务承诺函》，明确承诺为采购人建立专属技术服务通道、提供7×24小时应急响应支持及定期设备效能优化服务。若不提供视为无效磋商，由供应商承担相应法律责任。  3、能7×24通过远程、上门服务、电话、E-mail等方式为用户提供完善的售前和售后技术咨询服务；  4、接到故障通知，必要时成交供应商的认证工程师3小时内到达现场处理。  5、免费对用户进行使用前培训和维护培训，系统使用培训。  **付款条件：**  在合同签订后10个工作日内，成交供应商向采购人提交初步工作方案。采购人确认工作方案后，向成交供应商支付合同价款的70%。余款由采购人视工作开展、验收情况及预算执行情况支付（验收工作如需外聘专家，专家评审费由成交供应商承担）。  **其他要求：**  一、总体要求  1、供应商可根据项目要求，在响应文件中提出项目设计方案、实施方案（应包括人员安排、进度安排等内容）  二、验收要求及标准  1、根据采购需求的要求进行验收。  三、其它  1、报价必须含以下部分，包括：  （1）服务的价格；  （2）必要的保险费用和各项税金；  （3）其他[如运输、装卸、安装、调试、培训、技术支持、售后服务、更新升级等费用。 | | | |

**分标3 附件1：攻击诱捕工具技术需求**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标名称** | **技术要求** |
| 1 | 安全要求 | 产品完全基于KVM+docker架构，并在访问策略、进程、流量等方面采取严格的技术管控措施防止攻击逃逸，并且具备逃逸告警功能。（首次响应文件中提供产品界面功能截图证明材料） |
| 2 | 仿真数量 | 沙箱数量：≥4个同时在线；伪装代理：≥16个同时在线；诱饵：种类≥5种，数量不限。 |
| 3 | 沙箱仿真模块 | 应用服务类：支持wiki、bbs、discuz、ecshop、espcms、websphere、phpmyadmin、confluence、hadoop、crm、oa、tomcat、mailbox、jboss、zabbix、struts2、jenkins、weblogic、vpn、joomla等不少于20种高交互应用服务类沙箱。（首次响应文件中提供产品界面功能截图证明材料） |
| 系统服务类：支持ssh、redis、mysql、ftp、samba、memcahed、sqlserver、portcheat、momgoob、telnet、mysqlcheat、postgresql、ADB等不少于13种高交互系统服务沙箱。（首次响应文件中提供产品界面功能截图证明材料） |
| 数据仿真：新建沙箱时，向沙箱中注入脱敏数据，随机替换web服务的模板，增加沙箱的真实性。（首次响应文件中提供产品界面功能截图证明材料） |
| web沙箱联动：支持为web沙箱配置敏感目录，在该目录下随机生成普通配置文件、数据库配置文件、木马文件等；文件内包含其他沙箱的IP地址、用户名、密码等敏感信息。（首次响应文件中提供产品界面功能截图证明材料） |
| 沙箱支持调节行为灵敏度，开启或关闭流量阻断；支持自定义邮件告警级别；支持开启关闭溯源能力，自定义位置插入溯源组件。 |
| 4 | 诱饵感知模块 | 平台反制：支持制作Windows、Mac、Android反制木马，用户自定义上传反制程序并关联沙箱，伪造敏感信息，诱骗攻击者进行下载；其中Windows反制支持docx/doc/rtf/exe等4种类型；Mac反制支持dmg、pkg和app文件等3种类型；Android反制支持apk类型（首次响应文件中提供产品界面功能截图证明材料）  漏洞反制：支持git泄露反制、svn泄露反制、漏洞扫描工具反制、浏览器反制、网络代理工具反制、抓包工具反制、git clone反制等，攻击者无需下载并打开文件，访问沙箱或执行命令后即可在蜜罐系统上线。（首次响应文件中提供产品界面功能截图证明材料）  办公网诱饵：支持PC诱饵发布功能，通过agent在PC上发布与沙箱相关的虚假信息，包括网页浏览记录、网站登录密码、RDP连接记录、登录域凭据等。  文件诱饵：支持对已有文件word/excel/ppt加工，散布虚假信息到内网各处，感知攻击者访问行为。  邮件诱饵：支持向特定邮箱发送诱饵，感知邮件入侵行为。  互联网诱饵：支持Github与Gitee代码伪装服务，自动化发布代码项目至GitHub与Gitee网站。 |
| 5 | 智能蜜网模块 | 一键探测：支持一键感知探针感知节点所在网络的资产信息，分析当前网络状态。（首次响应文件中提供产品界面功能截图证明材料） |
| 一键关联：基于探测结果和智能算法，支持蜜网一键化部署，将探针节点自动关联至对应沙箱，快速形成欺骗蜜网，简化布防操作。（首次响应文件中提供产品界面功能截图证明材料） |
| 6 | 溯源反制模块 | 支持对黑客溯源功能，形成黑客溯源/黑客画像页面，溯源真人白名单标记，对溯源结果按照国内/国外/内网分类并展示，可提供对黑客备注功能。  支持分析黑客的身份信息和设备指纹信息，包括IP地址、社交网站真人身份、设备指纹、操作系统、浏览器等，支持不少于6种社交ID溯源能力。（首次响应文件中提供产品界面功能截图证明材料）  黑客画像支持展示攻击者身份、备注、源IP、内网/公网IP、浏览器信息，黑客轨迹聚合该黑客所有攻击事件，支持攻击源探测，探测攻击源的服务与端口。  具备windows攻击反制功能，可以反向控制攻击者设备，获取对方设备信息，进行交互式反制操作；可获取设备配置信息、网卡信息、IP信息、用户信息、进程信息、系统信息、桌面文件等；支持命令执行、文件上传下载、电脑截屏、摄像头拍照等操作，支持获取qq、wechat、手机号、Git、Email、iphone设备信息、浏览器保存的URL及对应的用户名等应用的用户ID、cobaltstrike、xshell、navicat等关键数据，便于身份溯源。（首次响应文件中提供产品界面功能截图证明材料）  具备Macos攻击反制功能，支持获取系统版本、内核版本、计算机名称、用户名、设备序列号、应用名称、应用版本、浏览器URL和用户名、微信账号、手机号、钉钉手机号、邮箱等关键信息; 支持命令执行、文件上传下载等操作。（首次响应文件中提供产品界面功能截图证明材料） |
| 7 | 行为记录模块 | 对于Windows沙箱的远程RDP攻击，支持录制攻击过程的视频，可回放攻击过程；  对于SSH沙箱的攻击，支持以视频的形式回放用户的命令行操作记录。  支持记录攻击者所有攻击行为，通过时间线展示，并可从攻击源、攻击手法、攻击资产、隔离沙箱、攻击类型、时间线等维度进行筛选查看。  支持记录各类Web应用与系统服务登录爆破，支持识别记录Web攻击类型，支持识别僵木蠕攻击、漏洞利用手法。  支持将不同攻击者对不同沙箱的攻击单独归并，分别展示为事件，可通过攻击事件回溯查看该事件所有攻击行为。  支持记录攻击者上传的任意文件，并分析其文件类型、MD5等判断其是否为恶意木马。  支持记录攻击者所有行为，并能识别真人与扫描工具。 |
| 8 | 服务要求 | 根据采购人实际需要，提供以下专业服务：  ▲1）现场服务：提供每年12次分析服务（每月1次）；  2）方案定制服务：通过网络环境调研，对蜜罐设备的部署位置、启用沙箱数量及种类、沙箱的仿真和交互程度等进行定制和优化，最大化发挥现有蜜罐设备的能力和价值。  3）动态运营服务：根据日常运营和实战攻防的不同阶段，抛出不同的蜜饵和仿真业务，通过动态变化的情报与反情报体系，保持蜜网的新鲜感和吸引力。  ▲4）成交后，采购人保留要求对设备性能及功能进行测试的权利，测试结果如果不满足本次采购要求，所投标产品视为无效采购人不予验收，并追究成交供应商相应法律责任。  以上服务内容，供应商须提供此项服务承诺函（格式自拟） |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分标：4** | | | | |
| **需求一览表** | 序号 | 标的名称 | 数量及单位 | 技术要求 |
| 1 | 全局无线设施联调和运维服务 | 1项 | 全局无线设施联调和运维服务（含广西统计局办公楼、中国统计资料馆广西分馆和广西统计资料中心博物馆所有办公区），服务内容包括：  ▲（1）提供相应设备，保障服务区域网络线路信号畅通。  （2）保障网络硬件设备实现无线联网运行。  （3）保障办公区域无线网络设备正常运行，提供无线网络硬件设备同等功能软件版本更新、升级，以及该软件版本配套的文档资料、用户手册；升级后用户将享有新版本软件的使用权利。  ▲（4）保障无线网络设备运行环境安全，包括无线网络硬件设备维保和管理终端平台软件升级、模块配置、技术支持等；当原无线网络硬件设备出现故障无法使用时，提供不低于原使用产品型号的备机进行替换保障。  ▲（5）无线网络设备日常故障排查、解除、保修物品收发，包含日常巡检响应，月度巡检，季度巡检和保养；提供至少2次/月的现场技术支持服务，运维内容包含技术培训、故障排查和保养。  ▲（6）提供URL库与应用识别规则库升级有效期，保证产品能及时更新发布的最新版本规则库。 |
| **商务条款** | **规范标准：**  采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。  **服务时间及地点：**  1、服务时间：自签订合同之日起1年。  2、服务地点：广西区内（采购人指定地点）。  **售后服务要求：**  1、免费维护至少1年（自交货并验收合格之日起计）；  2、能7×24通过远程、上门服务、电话、E-mail等方式为用户提供完善的售前和售后技术咨询服务；  3、接到故障通知，必要时成交供应商的认证工程师3小时内到达现场处理.  4、免费对用户进行使用前培训和维护培训，系统使用培训。  **付款条件：**  在合同签订后10个工作日内，成交供应商向采购人提交初步工作方案。采购人确认工作方案后，向成交供应商支付合同价款的70%。余款由采购人视工作开展、验收情况及预算执行情况支付（验收工作如需外聘专家，专家评审费由成交供应商承担）。  **其他要求：**  一、总体要求  1、供应商可根据项目要求，在响应文件中提出项目设计方案、实施方案（应包括人员安排、进度安排等内容）  二、验收要求及标准  1、根据采购需求的要求进行验收。  三、其它  1、报价必须含以下部分，包括：  （1）服务的价格；  （2）必要的保险费用和各项税金；  （3）其他[如运输、装卸、安装、调试、培训、技术支持、售后服务、更新升级等费用。 | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **分标：5** | | | | |
| **需求一览表** | 序号 | 标的名称 | 数量及单位 | 技术要求 |
| 1 | 信息系统等级保护测评 | 1项 | **一、总体要求**  依据《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）对上联国家统计局主干网(三级系统)等保测评服务；广西大数据应用统计支撑平台(三级系统)等保测评服务；广西第五次经济普查数据处理环境(三级系统)等保测评服务；工作信息网网站(二级系统)开展等保测评服务，并出具符合国家网络安全等级保护管理部门规范要求、公安机关认可的网络安全等级测评报告。  按照等级保护定级备案流程，协助开展定级备案工作，遵照等级保护基本要求，通过对系统的技术与管理的角度进行检查，如若信息系统未达到等级保护要求，需出具差距分析报告并协助整改，使信息系统符合等级保护的要求。  **二、依据标准**  《计算机信息系统安全保护等级划分准则》（GB 17859-1999)  《信息安全等级保护管理办法》（公通字[2007]43号）  《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）  《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 28449-2018)  《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）  《信息安全技术 网络安全等级保护测试评估技术指南》（GB/T 36627-2018）  **三、服务内容：**  **（一）安全咨询服务**  （1）安全培训服务  根据项目实际需要，进行安全技术培训。结合实际需求，进行信息安全等级保护政策、法规、技术标准等内容的安全培训工作，完成网络安全等级保护政策的宣贯、提高相关工作人员的信息安全意识、信息安全技能等。  （2）安全加固服务  依据《GB/T22239-2019信息安全技术网络安全等级保护基本要求》《GBT25070-2019 信息安全技术 网络安全等级保护安全设计技术要求》等相关标准要求，对本次项目涉及的服务对象进行安全等级化建设过程提供全过程督导咨询工作，并通过技术手段，对委托方的信息系统进行等级保护合规性、策略性配置和专项加固（非硬件类采购、非授权服务类采购）。  **（二）等级保护测评服务**  委托具有信息安全等级测评资质的第三方机构，依据《信息系统安全等级保护基本要求》（GB/T 22239-2019）等相关标准,对平台及信息系统的定级对象进行等级保护测评工作。  1、测评内容  ①安全通用要求  安全通用要求测评内容应包括安全技术和安全管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个方面的测评，安全管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理五个方面的测评。  ②安全扩展要求  应用了不同新技术的安全保护对象处于不同的应用场景中，面临不同的安全威胁，因此会有不同的安全需求，如本项目执行时发现等级保护对象涉及测评标准安全扩展要求（云计算、移动互联网、物联网、大数据、工业控制）方面内容的，则根据实际情况选定适用的安全扩展要求测评内容开展本项目测评工作。  ③在等级保护测评过程中，应采用访谈、检查、测试、工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。  ④对信息系统进行验证测试和渗透测试，检测包括但不限于SQL注入和跨站脚本等常见安全漏洞，并提供漏洞修补建议，及时采取适当的处理措施进行修补，有效阻止安全隐患被利用和发生安全事件。  ▲2、成果交付  测评完成后，出具符合国家网络安全等级保护管理部门规范要求、公安机关认可的网络安全等级测评报告，纸质版3份，电子版1份。  **四、成交供应商必须签署相关保密协议，严格遵守协议要求。**  **五、服务验收要求：**  在供应商和用户负责人双方同时在场情况下，用户对供应商提交的等级保护测评相关文档及最终交付物进行审核。在审核过程中，若发现有短缺或不符合项目需求、合同条款和质量标准的情况，供应商将负责补齐、修改并再次提交，由此引起一切费用由供应商承担。  **六、交付要求：**  本项目须根据网络安全等级保护测评要求，开展安全等级保护测评工作，测评完成后，提交有效的网络安全等级保护备案证明和出具符合等保2.0相关技术标准要求、国家网络安全等级保护管理部门规范要求,且公安机关认可的网络安全等级保护测评报告。 |
| 2 | 信息系统商用密码应用安全性评估服务 | 1项 | **一、总体要求**  依据《中华人民共和国密码法》要求和系统自身的安全需求分析，对上联国家统计局主干网(三级系统)；广西大数据应用统计支撑平台(三级系统)；广西第五次经济普查数据处理环境(三级系统)开展商用密码应用安全性评估服务，并出具符合商用密码测评管理部门规范要求、密码局认可的安全性评估报告。  **二、依据标准**  《信息安全技术 信息系统密码应用基本要求》（GB/T 39786—2021）  《信息系统密码应用测评要求》（GM/T 0115—2021）  《信息系统密码应用测评过程指南》（GM/T 0116—2021）  《商用密码应用安全性评估测评作业指导书（试行）》  《信息系统密码应用高风险判定指引》  《商用密码应用安全性评估量化评估规则》  **三、服务内容：**  **（一）安全咨询服务**  （1）安全培训服务  根据项目实际需要，进行安全技术培训。结合实际需求，进行商用密码应用安全政策、法规、技术标准等内容的安全培训工作，完成商用密码应用安全政策的宣贯、提高相关工作人员的信息安全意识、信息安全技能等。  （2）安全加固服务  依据《信息安全技术 信息系统密码应用基本要求》《信息系统密码应用测评要求》《信息系统密码应用测评过程指南》等相关标准要求，对本次项目涉及的服务对象提供全过程督导咨询工作，并通过技术手段，对委托方的信息系统进行商用密码应用安全合规性、策略性配置和专项加固（非硬件类采购、非授权服务类采购）。  **（二）商用密码应用安全性评估服务**  委托具有商用密码应用安全性评估资质的第三方机构，依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786—2021）等相关标准,对平台及信息系统的定级对象进行商用密码应用安全性评估工作。  1、评估内容  ①通用要求测评  核查信息系统中使用的密码算法、密码技术、密码产品和密码服务是否满足国家密码管理的相关标准或规范要求。  ②密码技术应用要求测评  具体包括物理和环境安全测评、网络和通信安全测评、设备和计算安全测评、应用和数据安全测评，验证不同安全等级信息系统的密码应用是否达到相应安全等级的安全保护能力、是否满足相应安全等级的保护要求。  ③安全管理测评  从制度、人员、实施和应急四个方面进行安全管理测评，验证信息系统安全管理机制是否完善，是否能够确保密码技术被合规、正确、有效地实施。  ▲2、成果交付  出具符合国家密码安全主管部门规范要求、区域相关密码局认可、符合商用密码安全技术标准要求的商用密码应用安全性评估报告，纸质版3份，电子版1份。  **四、成交供应商必须签署相关保密协议，严格遵守协议要求。**  **五、服务验收要求：**  在成交供应商和用户负责人双方同时在场情况下，用户对成交供应商提交的商用密码应用安全性评估相关文档及最终交付物进行审核。在审核过程中，若发现有短缺或不符合项目需求、合同条款和质量标准的情况，成交供应商将负责补齐、修改并再次提交，由此引起一切费用由成交供应商承担。  **六、交付要求：**  本项目须根据商用密码应用安全性评估要求，开展商用密码应用安全性评估工作，测评完成后，提交符合国家密码安全主管部门规范要求、区域相关密码局认可、符合商用密码安全技术标准要求的商用密码应用安全性评估报告。 |
| **商务条款** | **规范标准：**  采购标的需执行的国家标准、行业标准、地方标准或者其他标准、规范。  **服务期限及地点：**  服务期限：合同生效后，采购人通知进场之日起60个工作日之内完成。出具网络安全等级保护测评报告和商用密码应用安全性评估报告并验收合格后，服务结束。  服务地点：广西南宁市内采购人指定地点。  **付款方式：**  在合同签订后10个工作日内，成交供应商向采购人提交初步工作方案。采购人确认工作方案后，向成交供应商支付合同价款的70%。服务工作完成并出具测评报告后，采购人在10个工作日内向成交供应商支付合同余款（验收工作如需外聘专家，专家评审费由成交供应商承担）。  **其它要求：**  1、验收要求及标准：根据采购需求的要求进行验收。  2、供应商必须具备公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书；  3、成交供应商须独立承担并自行实施本项目的等级保护测评和商用密码应用安全性评估的全部工作。所有提交的正式测评报告（含最终报告、过程文档等要求盖章的报告）必须加盖成交供应商的法定名称章（公章）。测评服务（包括但不限于现场测评、报告编制、报告审核及盖章）属于本项目的核心服务内容，不得进行分包或转包。  4、合同签订后，成交供应商必须与采购人签订保密协议，以确保本项目建设的所有数据及资料保密安全。 | | | |