第四部分　采购需求说明书

“★、▲”号条款

《采购需求说明书》中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）则应答无效。标注“▲”号的条款为重要指标，负偏离（不满足要求）将导致技术得分的损失。

一、供应商服务要求

★1、注册地在广东省内或在广东省内有常驻服务机构。提供营业执照执照副本复印件或以供应商或其法定代表人名义签订的常驻服务机构租赁合同复印件或产权人为供应商或其法定代表人的服务机构的产权证明材料复印件。

★2、具备厂商北京启明星辰信息安全技术有限公司出具的针对本项目的原厂服务授权书或承诺书。授权书或承诺书内容中需包含在甲方指定的重要敏感时期提供应急/现场备机和现场技术支持服务的承诺。(投标时提供原件，或承诺在收到成交结果通知书 10 天内提供原件，未按要求提供的，采购人有权取消其中选资格)。

★3、近三年内，具备网络安全相关工作的实际项目经验。需提供合同关键页复印件，清晰显示合同签署日期、项目名称、网络安全相关（如防病毒、漏洞扫描、威胁防护等。

★4、服务商专职项目技术人员至少 1 人，必须具备信息安全或网络安全专业认证（注解 1）的其中一个认证；项目技术团队人员至少 2 人，且至少 1 人必须获得上述认证的高级认证（注解 2）的其中一个证书。

注解 1：INSPC、CISSP、CISP 系列、CCNA/CCNP/CCIE Security、HCIA/HCIP/HCIE-Security、H3CNE/HECSE/H3CIE-Secorityt、CISAW 等。

注解 2：CISSP、CISP 系列、CCIE Security、HCIE-Security、H3CIE-Security、CISAW 专家高级证书等。

项目技术人员需为常驻广州人员，对甲方的需求能及时响应并提供现场技术服务。当项目技术人员出现离职、长期休假等情况无法及时履行技术服务的情况时，乙方快速安排不低于合同要求的技术人员递补并按照合同要求提供相关技术服务。

二、项目需求内容

本项目向供应商采购安全维保服务，申请一次性谈定三年的价格标准及续签优惠折扣，本期合同签署一年。后续视项目的执行情况及我行的财务管理要求，若满足续签条件则按约定的优惠标准执行下一期项目，若不满足续签条件则重新评估项目情况。项目的验收方式及标准详见合同模板第四条验收和第五条付款。本项目服务内容详见下表：

2024-2025 年网络安全维护服务项目服务内容				
序号	服务项目	项目类型	服务要求	服务内容
1	入侵检测	入侵检测系统升级服务及运行检查	按周	每周 1 次对广东省分行 IDS 设备（启明星辰）现场提供 IDS 软件及特征库升级服务。根据甲方要求提供重要敏感时期的应急/现场备机保障服务。
		入侵检测系统策略定制	按季度	按甲方要求提供省行及辖内二级分行在用启明星辰 IDS 设备策略定制及优化的现场服务。
		入侵检测系统安全巡检服务，应急响应现场支持服务及其他等	按周	每周提供 1 次《中国银行内网安全日志分析报告-周报》；每周提供现场日志分析服务，并协助甲方排查和处理风险问题。
			按月	每月提供 1 次《中国银行内网安全日志分析报告-月报》
				紧急情况下提供每周 7x24 小时的安全应急响应服务及现场问题处理服务
2	漏洞扫描	内网设备漏洞检测,分析,评估并提供漏洞修补建议	按季度	按季度根据甲方要求对内外 IT 资产进行漏洞扫描（工具为启明星辰漏扫系统），对持续发现的漏洞提供解决方案或建议。每次扫描结束后提交《中国银行广东省分行主机漏洞扫描报告》并跟进，在文档中包括补丁升级报告及修复建议等。建立漏洞扫描台账，按风险级别（特高危、高危、中危、低危）对安全漏洞分级管理，在漏洞处置完成后，立即进行复测。扫描特征库应根据官网更新，并提供应急备机保障服务。
				每次扫描提交报告后安全服务商应提供不少于五个工作人天的工程师驻场分析响应服务。
				根据甲方要求对内网重要业务系统进行漏洞扫描检测，评估并提供优化建议
3	防病毒预警	防病毒巡检及应急处理服务	按工作日	梳理辖内行办公终端的病毒库（亚信）最新版本更新率情况，并根据甲方要求进行数据优化及问题处理
			按周	对防病毒服务器进行巡检服务。每周提供防病毒服务器运行报表，报表内容包括客户端病毒库升级情况统计；
				协助对每周前 10 名病毒发作次数最多的计算机处置
				协助对每周前 10 名严重病毒发作次数的计算机处置
			按月	每月提供防病毒服务器运行报表，报表内容包括客户端病毒库升级情况统计；
				协助对每月前 10 名病毒发作次数最多的计算机处置
				协助对每月前 10 名严重病毒发作次数的计算机处置

2024-2025年网络安全维护服务项目服务内容				
序号	服务项目	项目类型	服务要求	服务内容
				每月现场跟进处理前十严重病毒不少于三个工作日
		防病毒软件版本升级	甲方要求	协助实施防病毒软件版本升级，涉及防病毒软件有关的版本和组件升级。
		病毒预警及应急响应支持	按月	提供疑似病毒处置技术支持服务，病毒巡检发现若有严重病毒应提供工程师现场分析严重病毒处理办法，现场支持至严重病毒得到控制为止。
4	安全趋势分析	网络安全（信息安全）风险提示	按月	提供安全服务商网络风险提示文档1份；文档内容要求如下：服务商应收集全球网络安全风险信息，针对广东省中行网络情况给出网络安全风险提示，并给予相应建议和解决办法。
			甲方要求	在甲方重点保障时期提供安全情报分享服务，及时向甲方提供有助于提升安全防护能力的安全情报，若涉及问题处置，可提供现场支持服务，协助甲方完成问题修复
		半年度、全年度的安全趋势分析和报告	半年度	提供安全厂商半年及全年的服务状况，总结服务的内容和效果，给予详细的数据分析各个服务项目的发展趋势，针对中行存在问题给予相关的建议。并结合中行业务等信息提供全球网络安全介绍，提供相应的风险提示和建议。
				结合安全服务工作情况，每半年出具《中国银行广东省分行网络安全评估报告-半年报》

各项服务需求：

（一）入侵检测服务

1、入侵检测系统升级服务及运行检查

内容说明：针对广东省分行在用的入侵检测系统IDS（启明星辰品牌）所使用入侵检测系统的软件及特征库升级服务。协助产品厂商提供安全产品软件安装及升级，提供特征库的定期更新，确保相关产品特征库处于最新状态。

范围：启明星辰厂商的天阗入侵检测系统（省行3台，二级分行20台）；

次数：1次/周。

方式：升级文件必须为厂家官网发布，乙方安排工程师现场对特征库等更新，并确认产品运行状态良好，并在月巡检报告记录模块更新记录。

实施时间：每周第五个工作日内升级完毕。

此外，在甲方要求的重要敏感时期，服务商需协调厂家提供入侵检测系统IDS的应急/

现场备机保障服务。

2、入侵检测系统策略定制

内容说明：包括对全部在用入侵检测系统 IDS 的配置优化，系统策略制定等；协助制定符合省中行实际安全需求的运行策略；协助制定符合辖内二级分行实际安全需求的运行策略；制定相关的入侵检查系统策略提供 IDS 系统事件定期报表，详细分析 IDS 报表与报警事件，并根据实际环境确认事件危害级别，协助制定符合实际运行要求的检测策略；在已定义符合实际运行要求的 IDS 检测策略基础上，提供系统事件定期报表，详细分析 IDS 报表与报警事件，并根据实际环境确认事件危害级别，不断优化检测策略。

范围：现场服务：省行在用 IDS；远程服务：辖内二级分行；

次数：每季度 1 次。

方式：根据甲方要求在甲方现场针对省行及各个二级分行定制各自独立的策略。根据每个分行特定环境编写策略定制文档。待中行确认相关策略文档后，甲方安排工程师根据文档记录策略在天阗 IDS 添加各分行策略并下发到各个分行 IDS 引擎中。根据收集上来的数据再不断针对各个分行策略进行优化，相关优化策略均记录在策略文档中，并定期发送更新的策略文档给甲方。实施三个月后，根据优化策略文档更改现有运行策略。

实施时间：合同期每季度对策略进行全面调整。

3、入侵检测系统安全巡检服务，应急响应现场支持服务及其他等

内容说明：每周检查入侵检测系统日志，提供网络安全建议。每月检查入侵检测系统日志，提交安全分析月报。提供 7x24 小时的安全应急响应及现场服务、安全技术和动态的定期通报、解决产品本身配置问题、提供漏洞修补工作的建议、协助解决系统受到攻击的问题和安全隐患。提供定期巡检服务，巡检内容包括：入侵监测系统、漏洞扫描系统。对于其中发现的安全事件，需对高、中级别的安全事件提出详细的技术分析，评估事件造成的危害，分析 IDS 报警事件，根据不同事件类别，分析事件的详细技术细节，确认事件的危害情况；对审计出的重要安全事件，确认攻击与被攻击对象、事件成因、攻击原理、攻击结果、并提供应对措施和建议；提交巡检报告，协助追查攻击 IP 和确认相关处理结果。紧急情况下提供每周 7x24 小时的安全应急响应服务及现场问题处理服务。

内容技术细节：根据 IDS 报警事件类别提供相应的处理建议并提交报告，如有疑似威胁事件，需协助甲方跟进有关问题处理。

范围：现场服务：省行在用 IDS；远程服务：辖内二级分行；

次数：周报：1 次/周，每周不少于 1 个工作日人天的现场日志分析相应服务。月报：1 次/月，共 12 次/年。

（二）漏洞扫描服务

内容说明：采用网络漏洞扫描工具（启明星辰品牌），根据甲方要求每季度对内网 IT 资产进行一次漏洞扫描工作，并对扫描结果进行分类和形成报表，并提供建议修补漏洞。根据扫描工具提供的漏洞扫描与检测技术，快速、高效、准确地发现系统安全隐患并提供漏洞修补建议；若现有的扫描工具时效性无法满足进度要求，乙方需协调安排同样基线的扫描工具。

内容技术细节：识别各种操作系统和主机名称，包括但不限于各版本 Windows、Linux、Solaris、SCO Unix、HP Unix、IBM AIX、IRIX、BSD 等。支持的扫描对象包括各种终端、服务器、工作站、网络打印机以及相应的网络设备。扫描内容分类包括但不限于 Windows 共享类、 Web 服务类、CGI 类、信息搜集类、强力攻击类、守护进程类、电子邮件服务类、FTP 服务类、DNS 类、网络管理 SNMP 类、Proxy 类、协议欺骗类、RPC 类、NFS 类、NIS 类、后门类、网络设备类、蠕虫病毒类、缓冲溢出和拒绝服务攻击类、数据库类等。

范围：省行本部，辖内 20 家二级分行及 12 家广州管辖分支行及其辖内网点。

次数：1 次/季度（含复测）

方式：编写主机扫描预备文档，制定扫描时间、陪同人员、策略建议、部署要求等；文档经过甲方技术人员确认后，主机扫描系统中制定针对本次主机漏洞扫描策略；在预定时间内对目标主机进行主机漏洞扫描；收集主机扫描漏洞的数据，生成相应报告；协助中行系统管理人员修复扫描中发现的漏洞。扫描特征库应根据官网更新，并提供应急备机保障服务。

实施时间：

每季度一次扫描，报告于第二个月内提交，安全服务商工程师进行不少于五个工作日跟进处理，并与于第三个月前复测及处理。具体时间以甲方要求为准。

（三）防病毒预警服务

1、防病毒维护

内容说明：

每工作日协助甲方梳理办公终端病毒库更新情况；

每周协助甲方梳理防病毒数据统计信息；

每月协助甲方梳理防病毒软件防病毒数据统计信息；提供相关报表：

统计感染病毒主机的统计数据、按照病毒严重性排名、按照病毒出现次数排名；

针对每家分行内部病毒发作次数前十名电脑提供病毒分析，解决办法，源病毒主机列表等；

针对每家分行防病毒服务器严重危险报警次数前十名电脑提供病毒分析，解决办法，源病毒主机列表等；

针对每家分行防病毒客户端病毒库更新版本分布情况等；

针对中行内部病毒的前十名提供病毒分析，解决办法，源病毒主机列表等；

随报表提供相应的专杀工具，系统补丁；

提供各个杀毒厂商公布的流行病毒名称，并给予防范建议；

安排人员协助病毒主机修复情况。

提供 7*24 小时电话咨询服务，解决日常病毒查杀的相关咨询。

针对外界发表的严重病毒警告，提交《病毒预警文档》

针对爆发性病毒派专职工程师前往客户现场提供应急处理建议，并协助甲方处理紧急状况，直至问题解决。

范围：甲方全辖防病毒

次数：

日报：1 次/工作日，每工作日梳理内网终端病毒库更新率情况，并提供处置建议。

周报：1 次/周，每周不少于 1 个工作日人天的现场日志分析相应服务。

月报：1 次/月。

2、防病毒预警及辖内分行防病毒服务器技术支持服务

内容说明：每月对全辖防病毒服务器进行巡检；协助管理员维护日常防病毒服务器策略；协助管理员建立日常防病毒服务器报表模板；对防病毒服务日常维护提供远程技术服务。

范围：甲方全辖防病毒。

次数：1 次/月

方式：对地市行防病毒服务日常维护提供远程技术服务。

实施时间：根据地市行要求提供远程支持服务，不定期。

每月定期病毒巡检，发现若有严重病毒提交事件报告，并提供工程师现场分析严重病毒处理办法，驻场至严重病毒得到控制为止

（四）安全趋势分析

1、网络安全（信息安全）风险提示

内容说明：每月定期提供网络安全风险提示信息；收集权威金融同业网络安全（信息安全）信息，结合中行网络安全状况做案例分析并给予相应技术建议；定期收集金融行业应用系统漏洞信息并形成安全预警信息文档；针对以上信息并根据甲方具体要求做案例深入分析

及跟进处理。在甲方重点保障时期提供安全情报分享服务，及时向甲方提供有助于提升安全防护能力的安全情报，若涉及问题处置，需提供现场支持服务，协助甲方完成问题修复。

范围：广东省分行边界网络区域

次数：定期每月 1 次全年共 12 次，突发事件不计次数。

方式：如有重大网络安全风险，需提供《网络安全风险提示文档》

2、半年度、全年度的安全趋势分析和报告。

内容说明：根据项目执行情况，提供安全事件趋势分析文档，文档包括半年服务内容描述、可疑时间分析、年度常见事件汇总及解决建议、全球网络安全趋势分析。总结服务的内容和效果，给予详细的数据分析各个服务项目的发展趋势，针对中行存在问题给予相关的建议。并结合中行业务等信息提供全球网络安全介绍，提供相应的风险提示和建议。

范围：全辖内网。

次数：每半年一次

方式：现场技术服务。

（五）其他服务要求

1、重要时段现场支持服务

内容说明：根据甲方具体要求，提供技术工程师现场值班服务；按照甲方具体要求，在相关重要时段期间每天对在用 IDS 及防病毒系统进行报警事件收集和处理；临时对指定目标进行漏洞扫描并处理发现问题；对紧急突发网络安全事件协助甲方进行处理。

范围：全辖 IDS/CSP、防病毒系统、漏洞扫描工具

次数：甲方指定的重要时段。

方式：省行本部现场

实施时间：由甲方具体指定。

2、技术人员要求

能力要求：服务提供商应向甲方提供优质的技术团队，技术人员必须具备基础的信息安全认证资质（见第 1 页 注解 1），并尽可能安排高级认证技术人员（见第 1 页 注解 2）。

数量要求：专职项目技术人员至少 1 人，项目技术团队人员至少 2 人，且高级认证技术人员数量不少于 1 人。

时效要求：项目技术人员需为常驻广州人员，对甲方的需求能及时响应并提供现场技术服务。

人员冗余要求：当项目技术人员出现离职、长期休假等情况无法及时履行技术服务的情况时，乙方能够快速安排不低于合同要求的技术人员递补，按照合同要求提供相关技术服务。

三、验收方式及服务标准

合同验收方式及标准见合同模板第四条 验收。

四、付款

详见合同模板第五条 付款。