中国保险行业协会网络安全服务项目采购比选文件

第一章 投标邀请

一、项目基本情况

（一）项目名称：中国保险行业协会网络安全服务项目采购

（二）项目预算金额：人民币 20 万元

（三）采购内容：

序号	名称	数量	采购需求
1	网络安全服务项目	1 项	具体详见采购文件

（四）合同交货期限：合同签订后 7 个工作日内开始服务，期限一年。

（五）本项目是否接受联合体投标：□是 ■否。

二、参加比选的资格要求（须同时满足）

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）投标人不得被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单；

（三）供应商必须具有网络安全服务项目相关的技术服务能力；

（四）法律、行政法规规定的其他条件。

三、获取比选文件

详见比选公告。

四、比选单位递交比选文件时，必须提供如下证明资料：

（一）有效的营业执照或法人证书（复印件）；

（二）公司简介；

（三）法人授权委托书（原件）；

（四）被授权人身份证（原件及复印件）；

（五）供应商的资信证明：会计师事务所出具的最近一年度财务审计报告；

（六）依法缴纳税收的记录：最近半年内任意一个月的纳税有效凭据或相关部门出具的依法纳税有效证明文件，依法免税的，应提供依法免税的相关证明文件（复印件）；

（七）依法缴纳社会保障资金的记录：最近三个月内缴纳社会保障资金的有效票据凭证或由社保中心出具的缴纳社会保障资金的有效证明文件，依法免缴的，应提供依法免缴的相关证明文件（复印件）；

（八）参加本次采购活动前三年内，在经营活动中没有重大违法记录的声明（格式，原件，授权代表签字并加盖供应商公章）；

（九）原厂授权函及服务承诺函（原件及复印件）；

（十）比选文件要求或供应商认为必要的其他资格证明文件（复印件，加盖供应商公章）。

五、比选时间及地点：

（一）提交比选方案文件截止时间：2022 年 11 月 29 日 15 时 00 分（北京时间），逾期或不符合规定的比选文件恕不接受。

请供应商将密封好的有效比选书（正本一份、副本四份）、比选书电子版（一份）邮寄至：北京市丰台区丽泽平安金融中心 A 座

5层中国保险行业协会，联系人：王超，联系电话：010-66290204

（二）比选文件开启时间：2022年11月30日14时30分（北京时间）

（三）比选文件开启地点：北京市丰台区丽泽平安金融中心A座5层，届时请参选单位派授权人参加比选。

（四）评标方法和标准：综合评分法。

六、公告期限

自本公告发布之日起15个自然日。

七、联系方式

联系人：王超、刘坤

联系方式：010-66290204、66290493

地址：北京市西城区金融大街15号鑫茂大厦北楼7层

第二章 采购需求

一、项目概况

该项目为协会网络安全提供渗透检测、漏洞扫描、网站安全监测、安全基线检查和源代码审计等服务。

二、项目主要商务要求

标的提供的时间	合同签订后 7 个工作日内开始服务，期限一年
标的提供的地点	中国保险行业协会
投标有效期	从提交投标（响应）文件的截止之日起 90 日历天
付款方式	合同签订后支付 50%，验收合格后支付 50%。
验收要求	满足招标参数要求，按期提供所有技术报告，按期完成所有服务。
履约保证金	不收取

三、项目具体技术要求

序号	名称	数量	需求说明
1	渗透测试服务	7 个	**1.服务目标：**7 个系统，详见附件。 **2.服务标准要求：** 服务方在渗透测试服务实施工作完成后七个工作日内，安全服务实施人员须出具一份渗透测试报告，根据测试结果，渗透将针对每种威胁进行详细描述，描述内容须包括测试范围、过程、使用的技术手段以及获得的成果。安全服务实施人员还须结合测试目标的具体威胁内容编写解决方案和相关的安全建议，为客户管理员的维护和修补工作提供参考，包含复测。 测试完成后须出具如下报告：《XXX 系统渗透测试报告》。

			3.服务内容要求：渗透测试服务是由服务方安全服务实施人员模拟黑客的行为模式，采用黑客的漏洞发现和利用技术，以及尽可能多的攻击方法，对服务目标的安全性进行深入分析。服务方安全服务实施人员须通过智能工具扫描与人工测试、分析的手段，以模拟黑客入侵的方式对服务目标系统进行模拟入侵测试，识别服务目标存在的安全风险。 渗透测试服务内容须包括：信息收集类、配置管理类（HTTP 方法测试、应用中间件测试、信息泄露、异常错误等）、认证类（客户枚举、密码猜解、密码重置、密码策略测试等）、会话类（cookie 测试、session 会话测试等）、授权类（越权访问、路径遍历、任意文件下载、逻辑缺陷测试等）、数据验证类（SQL 注入、跨站脚本、代码注入、URL 跳转、文件上传测试等、输入输出校验绕过、数据篡改）、系统应用漏洞（溢出、0day 漏洞等）。 **4.服务工具要求：**服务方须应采用业界成熟的商业化软件或软硬件一体化的 WEB 应用弱点扫描器、数据库漏洞扫描系统、自动化渗透测试工具、半自动化渗透测试等工具进行安全检查，保证对目标系统无重大影响以及扫描结果的准确性和可信度。 **5.服务流程要求：** 服务方在内部测试流程前须经过客户授权后进行，安全服务实施人员须到达客户工作现场，根据客户的期望测试的目标直接接入到客户的办公网络甚至业务网络中。免去安全服务实施人员从外部绕过防火墙、入侵保护等安全设备的工作。

			一般用于检测内部威胁源和路径。 服务方在外部测试流程前须经过客户授权后进行，安全服务实施人员无需到达客户现场，须直接从互联网访问客户的某个接入到互联网的系统并进行测试。这种测试是应用于那些关注门户站点的客户，主要用于检测外部威胁源和路径。 服务方在黑盒测试流程前须经过客户授权后进行，黑盒测试须安全服务实施人员对除目标系统的 IP 或域名以外的信息一无所知的情况下对系统发起的测试工作，这种方式模拟黑客行为，了解外部恶意客户可能对系统带来的威胁。 服务方在白盒测试流程前须经过客户授权后进行，白盒测试则是指安全服务实施人员通过客户授权获取了部分信息的情况下进行的测试，如：目标系统的帐号、配置甚至源代码。这种情况客户模拟并检测内部的恶意客户可能为系统带来的威胁。
2	漏洞扫描服务	4 次	**1.服务目标：**协会全部网络系统及设备。 **2.服务期限：**一年，4 次。 **3.服务标准要求：** 服务方在完成漏洞扫描服务后，须出具《XXX 漏洞扫描报告》，报告须简要描述信息系统存在的安全漏洞及危害。扫描对象、扫描工具、扫描时间、漏洞分析（漏洞类型、漏洞所在页面、漏洞原理、漏洞利用、漏洞危害等）、加固修复建议、解决方案等。 服务方安全服务实施人员须提供现场服务。 **4.服务内容要求：**

			服务方对授权资产域名在互联网资产上开放的和内部未对外开放的，包括但不限于：子域名、IP 段、高危漏洞指纹信息、高危 POC 探测等资产等敏感信息进行搜集和梳理，并将互联网资产信息整理后交付中国保险行业协会。通过技术人员或相应系统设备对协会全部互联网应用系统和内部应用系统及设备实施安全扫描，对目标应用系统及设备的漏洞、用户名与口令、安全策略等方面进行评估，并对扫描报告进行分析并出具相应报告。并根据安全评估结果的具体情况，制定服务目标的加固建议，针对不同类型的目标系统，通过打补丁、修改安全配置、增加安全机制、建议添置安全设备等方法，合理加强服务目标的安全性。安全加固层面包括：设备层面加固、系统层加固、应用层加固。 **5.服务工具要求：** 服务方须应采用业界成熟的商业化应用漏洞扫描工具，帮助客户充分了解应用系统存在的安全隐患，建立安全可靠的应用服务，改善并提升应用系统抗各类应用攻击的能力（如：注入攻击、跨站脚本、文件包含、钓鱼攻击、信息泄漏、恶意编码、表单绕过等），协助客户满足等级保护、内控审计等规范要求。 服务方须应采用业界成熟的商业化数据库漏洞扫描工具，帮助客户充分了解数据库存在的安全隐患，通过定期数据库系统安全自我检测与评估,提升客户各类数据库的抗风险能力，服务方须为客户完成数据库建设成效评估，协助数据库安全事件的分析调查与追踪。

			服务方须应采用业界成熟的商业化远程安全评估工具，通过远程安全评估工具能够全面、深层次、快速的对客户 IT 资产所存在和潜在的安全风险进行评估，通过安全服务实施人员及设备所存在的安全风险一对一的修复建议指导客户对信息系统进行及时的正确性加固，使协会的信息系统抗攻击能力能够有效提升。减少、避免遭受被攻击的机率，从而提升信息系统整体安全性。 **6.服务流程要求：** 服务方须应采用业界成熟的商业化漏洞扫描工具对漏洞扫描服务范围内应用系统等进行网络层、系统层、数据库、应用层面的全面扫描与分析，扫描设备检测规则库及知识库须涵盖 CVE、CNCVE、CNVD、CNNVD 等标准。 服务方漏洞扫描服务完成后，须人工验证所发现的操作系统漏洞、数据库漏洞、弱口令、信息泄露及配置不当等脆弱性问题。提出准确有效的扫描报告，并针对漏洞扫描中出现的问题，提供解决方案，协助客户进行解决。
3	网站监测服务	10 个	**1.服务目标：**10 个域名，详见附件。 **2.服务期限：**1 年。 **3.服务标准要求：** 服务方提供云端 7*24 小时安全监测服务。 在不影响互联网应用系统正常运行的情况下，为其 web 应用系统提供 7*24 网站安全监测与预警服务。提供 7*24 小时的网页木马监测、网页篡改监测、网站可用性监测、网页关键字监测、Web 漏洞监测、钓鱼监测服务等。第一时间对监控

			对象的异常状态进行分析及告警。 提供《监测服务报告》，每月一次；《事件分析与处置报告》、《威胁情报预警》，按需触发，不限频次。 **4.服务内容要求：** 提供 7*24 安全威胁检测，由三级安全运营团队通过大数据分析、体系化关联规则、威胁狩猎、威胁情报等技术协助威胁分析和处置，实现威胁闭环管理。 服务过程中结合本地安全工具支持对挖矿活动、流氓软件、可疑文件、勒索软件、僵木蠕、Webshell 等 18000 种以上恶意程序实时检测。 针对主动或被动发现的安全事件提供响应和处置服务，对僵木蠕、Webshell、病毒、勒索病毒、挖矿病毒等各类安全事件快速处置，消除或减轻影响。 通过信誉库、安全事件库、网络资产库、威胁情报库、国内外开源/商用情报、威胁情报联盟共享等方式持续获取并更新威胁情报数据，及时为客户提供互联网上受影响的资产范围和清单。 对最新漏洞的原理、触发点、攻击事件 IOC 等进行深入分析，提供最优且影响最小化的安全加固建议，包括长期安全建设建议和临时缓解措施等可实施的方案。 支持通过可视化安全运营服务平台，查看当前安全状态，查看服务动态。 **5.服务工具要求** 服务期间以服务的形式提供一套支持软件化部署的资产发现

			与管理工具，可通过域名、IP 段、手工导入等多种途径对资产进行探测和管理，形成可维护的资产信息表。（提供相关证明材料）。 工具应提供 API 数据接口，支持与其他平台进行对接，实现本平台和其他平台的数据实时同步对接。（提供相关证明材料）。 服务期间以服务的形式提供一套支持漏洞扫描与管理工具，提供全面的漏洞扫描和跟踪清单。（提供相关证明材料）。 具备弱口令扫描功能，提供多种弱口令扫描协议，包括 SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS 等协议进行弱口令扫描，允许用户自定义用户、密码字典。 支持对 web 系统漏洞进行扫描检测，包括 SQL 注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞、隐藏字段、表单绕过、框架注入、0day 漏洞等。
4	安全基线检查及协助安全加固服务	4 次	**1.服务目标：**协会网络系统设备。 **2.服务期限：**一年，4 次。 **3.服务标准要求：** 服务方在完成基线检查服务服务后，须出具《XXX 基线检查服务报告》，须包括简要描述设备存在的安全配置缺陷及危害，对评估范围内相关设备进行手工检查。 基线检查服务报告须包括工作基本任务描述、工作相关人员、时间、地点、范围、内容等多方面内容，并对被检查信息安全配置进行客观的评价，对存在安全隐患或配置缺失的部分

			给出有针对性的安全修补建议。 **4.服务内容要求：** 服务方须根据协会工作需求，采用人工现场设备检查的方式对客户指定系统和设备等进行全面的安全基线检查服务，发现配置的不合规项,并结合行业实际需求提出系统整改建议，并协助进行安全加固，输出报告。 服务方基线检查服务内容包括但不限于以下内容： 检查对象和类型： 主机：WINDOWS、LINUX 等。 数据库：MSSQL、ORACLE、MySQL 等。 中间件：APACHE、WEBLOGIC、Tomcat、Nginx 等。 网络/安全设备：防火墙、路由器、交换机等。 主机安全检查： 业务系统涉及到的操作系统，如 Windows、Linux 等进行安全漏洞及安全配置缺陷的检查与评估。检测内容包括（但不限于）：身份鉴别方式、帐号安全设置、远程管理方式、多余帐号和空口令检查、默认共享检查、文件系统安、网络服务安全、系统访问控制、日志及监控审计、拒绝服务保护、补丁管理、病毒及恶意代码防护、系统备份与恢复、硬件冗余情况、硬盘分区格式等安全情况。 数据库安全检查： 业务系统涉及到的数据库，如 MySql、Oracle 等数据库系统进行安全漏洞及安全配置缺陷的检查与评估。检测内容包括（但不限于）：身份认证方式、帐号安全设置、管理权限和

			角色设置、多余帐号和缺省口令检查、数据库目录和文件系统安全、监听器管理设置、日志及监控审计、数据库版本和补丁管理、数据库备份策略、硬件冗余情况等安全情况。 网络设备配置检查： 对客户信息系统涉及到的网络设备，如防火墙、入侵检测（入侵保护）系统、路由器、交换机等进行安全漏洞及安全配置缺陷的检查与评估。检测内容包括（但不限于）：帐号安全设置、管理权限和角色设置、多余帐号和缺省口令检查、备份和升级情况、访问控制、路由协议、日志审核、网络攻击防护及端口开放、远程访问等安全情况。 中间件安全检查： 对业务系统涉及到的中间件，系统包括：weblogic、apache、Tomcat、Nginx 等进行安全漏洞及安全配置缺陷的评估。检测内容包括（但不限于）：系统和中间件的可用性、系统和中间件的完整性、系统中间件和应用的性能、通过与系统使用中关键人员的访谈来评估系统整体要求、对系统结构及运营架构进行高层面的评测、定位系统的运作流程中潜在的风险区域、产生基于中间件的最佳应用准则的建议报告等。
5	代码审计服务	2 次	**1.服务目标：**2 个系统，详见附件。 **2.服务标准要求：** 服务方在代码审计服务实施工作完成后七个工作日内，安全服务实施人员须出具一份代码审计报告，根据审计结果，将其发现的代码脆弱性、安全缺陷、编码安全规范行等面临的威胁问题，提供给开发人员修复，并须出具《XXX 系统代码

			审计报告》。 服务方安全服务实施人员须提供现场服务。 **3.服务内容要求：**代码审计服务是由服务方安全服务实施人员通过工具或人工针对目标应用系统的源代码，通过了解其业务系统，从应用系统结构方面检查其各模块和功能之间的功能、权限验证等内容；从安全性方面，检查其脆弱性和安全缺陷，对更新编码安全规范性和从源头上保障业务系统安全性。

第三章 评分标准

序号	评分内容	明细内容	分值	评分标准
1	价格部分（10 分）	投标报价	10	（1）评标基准价：满足招标文件要求且投标价格最低的有效投标报价为评标基准价。 （2）投标报价得分=（评标基准价/投标报价）×100×10%
2	商务部分（20 分）	服务能力相关证书	10	1、提供《信息安全服务资质认证证书》信息安全运维服务资质须符合三级及以上服务资质要求，提供证书复印件得 2 分，不提供不得分。 2、提供《信息安全服务资质认证证书》信息安全测评服务资质须符合二级及以上服务资质要求，提供证书复印件得 2 分，不提供不得分。 3、提供 ISO20000《信息技术服务管理体系认证证书》资质证明文件复印件得 2 分，不提供不得分。 4、提供 ISO27001《信息安全管理体系认证证书》资质证明文件复印件得 2 分，不提供不得分。 5、提供 ISO9001 质量管理体系认证证书证明文件复印件得 2 分，不提供不得分。 以上需提供复印件加盖公章，未提供不得分。 提供文件为原厂服务商资质文件的，需提供原厂服务商授权函及服务承诺函，未提供不得分。
		近三年业绩	6	近三年（2019 年 11 月 1 日至今）承担的类似项目业绩，每提供一项业绩得 2 分，本项最高得 6 分。 注：以上业绩需提供合同复印件，合同复印件需至少包括合

				同的甲乙双方、主要内容、双方签章及生效时间。未按上述要求提供不得分。
		服务能力相关材料	4	参加过安全运维类或安全保障类活动并获得用户方表彰的，每提供 1 个证明材料得 1 分，最高得 4 分。
3	技术部分（70 分）	技术方案	25	技术方案须符合 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》及本项目特点，根据协会信息系统整体的实际情况、契合度方面进行综合评价，最高得 25 分，技术方案包括但不限于： 1、《渗透测试服务技术方案》 2、《漏洞扫描服务技术方案》 3、《网站监测技术方案》 4、《安全基线检查及协助安全加固技术方案》 5、《代码审计服务技术方案》 每提供一项技术方案得 5 分，每缺少一项技术方案扣 5 分，扣完为止，不提供技术方案不得分。
		技术方案合理性	10	1、整体方案先进、能提供风险计算方法，方案合理可行，得 10 分； 2、整体方案描述较完善，方案较合理较可行，得 8 分； 3、整体方案描述基本完善，方案基本合理基本可行，得 5 分； 4、整体方案描述不够完善，方案不够合理不够可行，得 3 分； 5、整体方案描述不完善，方案不合理不可行，得 1 分； 本项未提供，得 0 分。

		项目组人员配备	5	**拟派项目经理（5 分）** 参与本次项目的安全服务项目经理须同时具备以下五种认证中的任意两种认证，所有人员提供有效证书复印件、身份证复印件及近 3 个月社保缴纳明细（人员社保缴纳单位须与投标人或原厂服务商名称一致），每提供一项得 1 分，最高得 5 分，要求投标文件中出具证书人员与用户现场实施人员为同一人，并提供承诺函，不提供不得分。 1、由中国信息安全测评中心颁发的《注册信息安全专业人员（CISP）》认证证书； 2、由中国网络安全审查技术与认证中心（CCRC）颁发的《信息安全保障人员认证证书（风险管理专业级）》； 3、由中国网络安全审查技术与认证中心（CCRC）颁发的《信息安全保障人员认证证书（应急服务专业级）》或《网络安全应急响应工程师证书》； 4、由公安部第一研究所颁发的《信息安全等级保护安全建设专业技术人员证书》； 5、由工业和信息化部颁发的《高级网络信息安全工程师》或《高级网络工程师》认证证书。
			10	**拟派项目组人员（10 分）** 参与本次项目的安全服务人员须具备由中国信息安全测评中心颁发的《注册信息安全专业人员（CISP）》认证证书或公安部第一研究所颁发的《信息安全等级保护安全建设专业技术人员证书》，提供有效证书复印件、身份证复印件及近 3 个月社保缴纳明细（人员社保缴纳单位须与投标人或原厂

				服务商名称一致），要求投标文件中出具证书人员与用户现场实施人员为同一人，并提供承诺函，不提供不得分。 1、岗位设置合理，岗位职责明确，与项目实施具体内容相匹配，人员数量满足采购需求，有利于保障项目实施，得 10 分； 2、岗位设置较合理，岗位职责较明确，与项目实施具体内容较匹配，人员数量较能满足采购需求，较有利于保障项目实施，得 8 分； 3、岗位设置基本合理，岗位职责基本明确，与项目实施具体内容基本匹配，人员数量基本能满足采购需求，基本利于保障项目实施，得 5 分； 4、岗位设置不够合理，岗位职责不够明确，与项目实施具体内容不够匹配，人员数量不够满足采购需求，较不利于保障项目实施，得 2 分； 5、岗位设置不合理，岗位职责不明确，与项目实施具体内容不匹配，人员数量不能满足采购需求，不利于保障项目实施，得 1 分； 本项未提供，得 0 分。
		工作质量目标及保障措施	10	1、项目质量目标分解、规划合理，项目质量控制体系健全，质量控制手段先进完善，对本项目针对性强，得 10 分； 2、项目质量目标分解、规划较合理，项目质量控制体系较健全，质量控制手段较完善，对本项目针对性较强，得 8 分； 3、项目质量目标分解、规划基本合理，项目质量控制体系基本健全，质量控制手段基本完善，对本项目基本有针对性，

				得 6 分； 4、项目质量目标分解、规划不够合理，项目质量控制体系不够健全，质量控制手段不够完善，对本项目不够有针对性，得 3 分； 5、项目质量目标分解、规划不合理，项目质量控制体系不健全，质量控制手段不完善，对本项目没有针对性，得 1 分； 本项未提供，得 0 分。
		工作进度计划及保障措施	10	1、工作进度计划详细，完全满足进度要求，安排合理，保障措施有力，得 10 分； 2、工作进度计划较详细，较能满足进度要求，安排较合理，保障措施较有力，得 8 分； 3、工作进度计划基本详细，基本能满足进度要求，安排基本合理，保障措施基本有力，得 6 分； 4、工作进度计划不够详细，不够能满足进度要求，安排不够合理，保障措施不够完善，得 3 分； 5、工作进度计划不详细，不能满足进度要求，安排不合理，保障措施不完善，得 1 分； 本项未提供，得 0 分。

附件：主要应用系统清单

序号	应用系统	网址
1	门户网站	http://www.iachina.cn
2	人身险产品信息库	http://tiaokuan.iachina.cn
3	财产险产品注册平台	http://cxcx.iachina.cn https://zcz.iachina.cn
4	财产险纯风险保费查询	http://cfxbf.iachina.cn
5	信息披露系统	http://icid.iachina.cn http://icidp.iachina.cn
6	独立董事人才库	https://dudongku.iachina.cn https://talents.iachina.cn
7	统计信息系统	https://stats.iachina.cn