上海黄金交易所网络安全专业服务采购书

一、项目情况

1. 项目名称：上海黄金交易所网络安全专业服务。
2. 采购需求：详见附件2。
3. 投标金额：小于人民币80万元（含税）。投标金额包含投标人为提供本合同项下所有服务所涉及到的所有费用，如税费等。
4. 投标保证金：人民币16000元。
5. 中标方式：根据本采购书“评分标准”对各投标文件进行评分，总分最高的投标人为第一中标候选人；总分相同的，较早投标者中标候选排序在先。
6. **投标有效期：从提交投标文件的截止之日起算不少于90天。**

二、商务要求

1. 投标人必须是在国内注册的独立法人，并具有相关经营资质。
2. 付款方式：

   项目将按进度分批次结算。

   ①、合同签订后支付50%；

   ②、服务完成，支付合同金额50%。
3. 投标金额为含税金额，包括提供本服务所有税费。本项目需开具增值税专用发票，如所提供的服务税率不同，须按照相应税率分别开具发票（合同金额不变）。
4. 投标人须提交投标保证金，投标文件中应附有投标保证金的付款有效凭证复印件。
5. 开标后投标人在投标有效期内撤回投标；或因投标人的原因对本次招标工作造成较严重后果的；或投标人在中标通知书发放后10天内不与招标人签订合同的，招标人有权不予退还投标保证金，且取消相关投标人的中标资格。
6. 本项目不支持联合体投标，本项目不得转包或分包。

7．招标过程中投标人如存在作假或舞弊行为的，或中标人在履约中存在违约行为的，一经核实招标人有权要求其两年内不得参与招标人系统内任何招标采购项目，如给招标人造成损失，须进行赔付。

8．投标人参与投标表示同意上述所有条款。

三、响应文件

响应文件应由：商务报价文件，商务响应文件（证明其为合格服务商的有关资格证明文件，采购文件要求提供的其他资料），技术响应文件（针对本项目的技术或服务偏离说明表，采购文件要求提供的其他资料）。

1. 响应人的商务报价文件至少应包括以下内容（均需加盖公章）

① 报价单（**单独密封**）。

2. 响应人的商务文件（均需加盖公章）

响应人提交的证明其有资格进行投标且有能力履行合同的资格证明文件应包括下列文件（未提供相应材料或材料无效者以废标计）：

① 法人授权委托书（格式见附件1），法定代表人及授权委托人的身份证（原件复印件，扫描打印件无效。）；

② 提供通过年检有效的企业法人营业执照、税务登记证、组织机构代码证；或上述证件的三证合一件，以上均为加盖公章后的原件复印件，扫描打印件无效。

③ 投标保证金的付款有效凭证复印件。

投标保证金应当从投标人的基本账户转出，并写明账户信息，如开户行以及账号等，并在银行付款备注栏中注明该投标保证金所对应的项目名称。

上金所账户信息：

单位名称：上海黄金交易所

开户银行：中国工商银行浦东分行

账号：1001280909000000163

④ 提交针对商务要求的响应。

针对商务条款响应表参考格式如下：

商务条款响应/偏离表

响应人名称：

序号	商务条款	响应	是否偏离	说明

响应人代表签字：_____（盖章）

⑤ 其他响应人认为有必要提供的资料。

*以上材料未全部提供或未按要求格式提供（特别标注的除外），以废标计。

3. 响应人的技术文件（均需加盖公章）

① 投标人本次服务服务方案。

② 响应人提交的针对招标需求及评分标准的响应，请逐项列明。参考格式见下表：

规格、技术参数响应/偏离表

响应人名称：

序号	招标要求	投标规格	响应/偏离	备注

响应人代表签字：_____（盖章）

③ 其他响应人认为有必要提供的资料。

4. 响应文件要求

响应人的响应文件必须按照采购书要求制作，**报价文件务必单独密封**。

四、评分标准

评分标准详见附件3

五、采购程序安排

1. 递交投标文件截止时间

2021年4月8日16：00前，响应单位将响应文件加盖公章并密封后(一式3份，

正本1份，副本2份)并附联系人名片，**送至上海黄金交易所采购办**（上海市黄浦区中山南路669号9楼），接收人：郭大伟，021-33128867。请附上联系人名片。

2. 投标人须根据招标人要求提交投标文件的电子版本。

上海黄金交易所

2021年3月30日

附件 1：

法定代表人授权书

本授权书声明：注册于*国家或地区的名称*的*公司名称*的*法定代表人姓名、职务*代表本公司授权*单位名称*的*被授权人的姓名、职务*为本公司的合法代理人，参加“*项目名称*”项目的投标及合同签订执行，以本公司名义处理一切与之有关的事务。

本授权书于 2021 年　月　日签字生效，特此声明。

法定代表人签字：_____

代理人（被授权人）签字：_____

单位名称（盖章）：_____

注：投标时须提交本授权书的原件，其中法定代表人和被授权人签字、公司盖章为必填项，否则将被视为无效授权，所投标书以废标计。

附件 2：采购需求

一、需求概述

拟采购一家网络安全厂商的专业技术服务。从信息系统安全评估；信息系统安全监测与保障；安全咨询、培训与宣传教育三方面，协助上金所做好信息系统安全技术防护工作，提升上金所网络安全保障能力。

服务期限为期一年。

二、需求内容

2.1 信息系统安全评估

2.1.1 应用系统风险评估

针对交易所的重要应用系统进行应用风险评估，尤其是新开发的应用或面向互联网应用，对应用进行全面化、专业化的安全评估，分析应用的系统安全架构和应用安全配置，发掘应用系统安全风险隐患，通过风险分析，提供安全防御与修复建议，以确保应用风险降低到可接受的水平。

2.1.2 系统脆弱性发现与评估

对交易所信息系统，包括：网络设备、安全设备、主机设备、数据库等，定期开展脆弱性扫描，发现系统中的安全漏洞，评估漏洞的影响性与危害性，并针对性地提出修复建议与修复优先级，以防止系统遭受已知漏洞的利用或攻击。

2.1.3 应用系统渗透测试

对交易所信息系统，特别是面向互联网的信息系统，定期开展黑盒测试，尝试漏洞挖掘和模拟攻击。通过完全模拟真实网络环境中黑客攻击的过程和方法，以求尽可能暴露并利用应用系统存在的脆弱性，并提供针对性的修复建议。

2.1.4 APP 系统安全评估及违规收集个人信息检测

针对交易所 APP 客户端和服务端进行安全评估与测试，查找 APP 系统可能存在的安全问题，对发现的问题予以验证，并提供针对性的安全修复建议。

通过各种技术手段，对交易所 APP 系统进行合规性检查，判断是否系统是否存在违规收集个人信息问题，并提供专业的整改建议。

2.2 信息系统安全监测与保障

2.2.1 互联网系统安全监测

针对交易所官方网站或指定互联网站点进行多方面的实时监控，一旦发现异常情况，第一时间通知相关人员，主要包括：

内容完整性的监测，如：网站的恶意挂马监测，网页篡改监测，敏感信息监测等；

域名监测，实时监测各地主流 ISP 的 DNS 服务器对交易所域名的解析状态；

钓鱼网站监测，监测针对交易所网站或其他站点的恶意仿冒站点。

2.2.2 安全检查及日志审计

定期采集交易所安全设备的日志，通过审计系统结合人工检查的方式予以综合性的检查与分析，以发现潜在的安全问题。

2.2.3 安全配置核查

定期检查安全设备的系统软件和安全配置情况，避免设备系统软件漏洞和配置不当所带来的安全风险，保障安全设备自身的安全性。

2.2.4 安全通告

定期通告信息系统的漏洞预警信息，分享行业内的安全形势与发生的重大事件。遇到出现重大信息系统安全漏洞或者事件时，第一时间通告交易所，并为紧急修复与处置工作提供专业的技术支持。

2.2.5 安全应急响应处置

当交易所发生重大信息系统安全事件时，第一时间提供技术支持，参与调查与处置工作，消除安全问题，将安全事件的影响性降低到最低程度，并提供整改建议，避免相同安全事件的再次发生。

2.2.6 重大活动驻场保障

在国内重大活动开展期间或者在交易所受到外部安全威胁情报时，提供专业安全保障人员驻场，弥补甲方安全技术人员的不足，加大对交易所网络安全状态的监测，并于第一时间处置安全问题，确保交易所的信息系统安全。

2.3 安全咨询、培训与宣传教育

2.3.1 安全咨询

为交易所的日常运维、系统建设提供专业的安全咨询服务，以弥补交易所安全技术人员在某些安全技术领域的不足。

2.3.2 安全交流与培训

与交易所安全技术人员定期交流行业信息安全形势，分享新的安全技术实践。并为交易所业务部门员工提供安全意识类的培训；为交易所技术人员提供技术类安全意识培训；为交易所安全技术人员，提供安全专业技术培训。

2.3.3 安全宣贯

定期向交易所提供各类安全意识或活动的宣传类文案，包括并不限于，宣传海报、公众号文案、定制化的安全宣传手册等。协助交易所安全技术人员组织好各项安全宣贯活动。

三、级别要求

服务期限一年。

序号	服务项	频率要求	响应要求	备注
1	应用系统风险评估	提供不少于 4 次	接交易所通知后 3 个工作日内响应	应用系统范围不限
2	系统脆弱性发现与评估	提供不少于 6 次	接交易所通知后 3 个工作日内响应	信息系统范围不限
3	应用系统渗透测试	提供不少于 10 次	接交易所通知后 3 个工作日内响应	应用系统范围不限
4	APP 系统安全评估及违规收集个人信息检测	提供不少于 4 次	接交易所通知后 3 个工作日内响应	
5	互联网系统安全监测	实时提供	无	
6	安全检查及日志审计	提供不少于 12 次	接交易所通知后 3 个工作日内响应	
7	安全配置核查	提供不少于 4 次	接交易所通知后 3 个工作日内响应	
8	安全通告	每周 1 次例行通告，重大风险提示第一时间通告	无	
9	安全应急响应处置	按交易所需求提供	接交易所通知后 2 小时内提供安全技术支持响应	
10	重大活动驻场保障	提供驻场保障服务人天不少于 60 人天	接交易所通知后 3 个工作日内响应	

11	安全咨询	按交易所需求提供	接交易所通知后 3 个工作日提供安全咨询响应	
12	安全交流与培训	提供不少于 3 场次	接交易所通知后 5 个工作日内响应	
13	安全宣贯	不少于 12 次	无	

附件 3：评分标准

项目评分标准

一、评标原则：

1、采用“百分制评标法”，分别对技术需求与商务需求进行评分。

2、对所有投标人的投标评估，评委都采用相同的程序和标准。

3、合并投标人后，有效投标不足 3 家，本次招标做流标处理。

4、对采购书及评分标准的理解出现争议时，其最终解释权在招标人。

5、若所有的有效投标经评分后商务技术得分大于等于 39 分的投标少于 2 家，本次招标做流标处理。

二、符合性检查：

凡出现下列情况之一者，予以废标：

1. 投标人未提交投标保证金或金额不足、投标保证金形式不符合招标要求的；
2. 投标书未按招标文件所附格式或者招标文件所提要求提供各类文件者；
3. 投标材料未按照招标要求加盖公章，或法定代表人（法定代表授权的代理人）签字；
4. 代理人无法定代表人出具的授权委托书；或没有出具清晰可辨的法定代表人和代理人身份证复印件者；
5. 超出经营范围投标的；
6. 投标有效期不满足要求的；
7. 投标文件未能满足本采购书**“商务要求”**、**“响应文件”**要求及本采购书附件 2 **“采购需求”**要求全部条款者；
8. 投标总价格大于或等于 80 万元的；
9. 递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标内容报有两个或多个报价，且未声明哪一个为最终报价的（按采购书规定提交备选投标方案的除外）；
10. 附加条件的报价（除采购书中有规定外）；
11. 投标人虚假投标，提供的投标文件与事实不符；或在澄清过程中虚假澄清，提供的澄清文件与事实不符；
12. 开标后，投标人提出降价或进行抬价或利用澄清机会实质性变更投标价的；
13. 投标人复制采购书的技术规格相关部分内容作为其投标文件的一部分的；
14. 不同投标人投标文件有雷同现象的或者不同投标人的投标保证金来自同一机构的（以上情况相关投标均为废标）；
15. 招标过程中投标人存在作假或舞弊行为的；
16. 有其他违法违规情形的或符合采购书规定的其他废标条件的。

三、评标标准

本招标评标采用综合评分法，满分为100分：其中价格分为35分，商务技术分为65分。

对本次招标中涉及的各项评分因素分数之和为综合得分;综合得分按照由高到低排序并作为中标候选人选用顺序，出现得分并列时，按照投标时间先后排序中标候选。

如某投标人投标总价低于全部通过符合性审查投标人报价均价的比例超过26.11%（含）需在3个工作日内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应投票表决是否将其作为无效投标处理。

四、价格评分

符合招标文件要求的为有效投标。所有有效投标人中最低投标价格作为评标基准价，其得分为满分（35 分），其他有效投标报价得分计算公式如下：

投标价格得分=（评标基准价/投标报价）*35

五、商务技术评分

为使评分时能体现量化，评委按以下内容进行评定后打分，各项得分合计后计算算术平均值后为各投标单位的最终得分。

评标要素	评分项	分值
用户案例	自2018年1月1日以来，投标人为企业提供网络安全专业技术服务的用户案例，根据案例的规模和交易所业务相似度，每个案例0-1分，最多提供12个案例。（需提供合同扫描件或复印件，要求清晰显示服务内容、项目金额、项目时间等主要项目要素，并加盖公章） *合同须为投标人签署，其子公司合同不得分;合同无签署日期不得分。	12
资质证书	投标人具备较强的网络安全应急服务能力；具有国家互联网应急中心（CNCERT）颁发的网络安全应急服务支撑单位证书，国家级得3分，省级得1分;国家互联网应急中心2020年度对支撑单位考核结果为优秀得2分，良好得1分。（需提供资质证书扫描件或复印件及评优证明材料）	5
	投标人具备较强的安全漏洞挖掘能力，具备国家信息安全漏洞库（CNNVD）一级技术支撑单位得5分，具备二级技术支撑单位证书得3分，具备三级技术支撑单位证书得1分；无证书不得分。（需提供证明文件）	5
技术能力	1、自2018年1月1日以来，投标人在国家信息安全漏洞共享平台(CNVD)漏洞提交数量： A、30000≤漏洞提交数量，得8分； B、25000≤漏洞提交数量＜30000，得6分； C、20000≤漏洞提交数量＜25000，得4分；	8

	D、漏洞提交数量＜20000，得 2 分。 ＊需提供国家信息安全漏洞共享平台官网（https://www.cnvd.org.cn/)每月漏洞信息月度通报关键页截图(含归属月份、报送单位、上报数量等），提交数量由每月累加计算，提交单位名称必须与投标人名称一致，未按要求提供材料的不得分。	
	2、自 2018 年 1 月 1 日起检测出各类软件及系统的漏洞数量并得到国家互联网应急中心（CNCERT）、国家信息安全漏洞库（CNNVD）或国家信息安全漏洞共享平台(CNVD)认可，每提供 3 个 CNVD 或 CNNVD 号可得 1 分，最多 15 个。（需提供证明文件）	5
服务方案	1、投标人备有完善的服务方案，方案中，组织计划严谨、服务内容清晰，人员结构合理的得 0-3 分，本项 0-3 分。	3
	2、方案中详细描述信息系统安全评估服务计划安排，内容至少包括技术服务人员组成、评估方式方法、评估技术工具清单等，视其合理性、有效性及贴合需求程度，得 0-3 分，本项 0-3 分。	3
	3、方案中详细描述信息系统安全监测与保障服务计划安排，内容至少包括监控保障人员组成、监控技术方法、保障工作计划，应急响应处置流程等；视其合理性、有效性及贴合需求程度，得 0-3 分，本项 0-3 分。	3
	4、方案中详细描述安全咨询、培训与宣传教育计划安排，内容至少包括咨询范围、培训形式、宣贯方式等；视其全面度及与需求的贴合度，得 0-3 分，本项 0-3 分。	3
	5、方案中详细描述本次服务项目中拟投入的技术工具或设备等；依据提供的工具或设备的数量、适用性、针对性得 0-3 分； 投入的技术工具或设备等为自主研发的，视其数量及重要度，得 0-2 分（需提供计算机软件著作权登记证书）。	5
项目人员	1、投标人针对本项目提供的项目经理须满足正规高等院校全日制本科及以上学历、并具备 5 年以上信息安全从业经验和类似项目相关技术服务团队管理经验,视其工作经验相关度及丰富度，得 0-3 分。投标人针对本项目提供的项目经理具备信息安全类证书如 CISP 等或项目管理类证书如 PMP 等有效认证证书进行综合评分，得 0-2 分。（需提供项目经理资质、经验、投标人为其缴纳社保等证明文件） ＊ 中标后项目经理员需与投标文件保持一致，不得更换。	5
	2、投标人针对本项目所提供技术服务人员均需满足两年以上类似项目的从业经验，视提供的现场服务人员数量、资质水平、案例经验，得 0-3 分。（需提供服务人员资质、经验、社保等证明文件） 投标人须对其长期服务能力和后备人员储备培养等情况说明,视其人员储备规模及人员培养力度，得 0-2 分。 ＊ 中标后服务人员需与投标文件保持一致，不得更换。	5
增值服务	投标人在本项目招标需求的基础上，提出个性化、超级别的服务，根据服务的价值进行评分，得 0-3 分。	3

注：1、每一评分项均不重复得分；

2、因具有资质、证书等原因得分的，投标人须提交清晰的资质或证书的原件扫描复印件（其他证明文件无效），否则不予得分；