**关于信息安全测评服务项目立项及单一来源采购**

**相关事宜的请示**

公司领导：

公司eMAS2.0项目和再·型-地震巨灾模型2.0项目即将上线对外提供服务，其中，eMAS2.0项目的苹果交易场景更是涉及到资金流动，为保证资金安全及为防止因应用层面的漏洞造成来自外部的非法访问和恶意攻击等事件的发生，有必要采购专业的安全评测服务，完成对应用系统的渗透测试、代码审计、安全加固等工作任务。申请项目立项（详见附件一：信息安全外包服务项目立项报告），具体请示内容如下：

1. **项目必要性及可行性**

eMAS2.0项目和再·型-地震巨灾模型2.0项目，作为对外提供服务的信息系统，面临的信息安全风险更高，监管对这类系统的安全要求也更高。eMAS2.0项目的苹果交易场景更是涉及资金流动，为保证交易资金安全、为提高该类系统安全性及稳定性，防止来自外部的非法访问和恶意攻击，有效预防信息安全风险的发生，需要对相应的业务系统开展渗透测试、代码审计等专业安全评测。渗透测试、代码审计等安全评测是专业安全公司的常规外包服务主要内容之一，这些专业安全公司组建了成熟的、专业能力强的技术团队，长期服务于各大金融机构。

1. **项目内容**

**渗透测试：**渗透测试是指由信息安全工程师利用安全工具并结合实践经验，同时采用各种攻击技术对系统进行非破坏性质的侵入测试和模拟黑客攻击。这种测试方法可以非常有效的发现最严重的安全漏洞，尤其是与全面的代码审计相比，其更高效。渗透测试主要包括：信息收集类（互联网可收集到高价车定价系统的敏感信息），配置管理类（HTTP方法测试、应用管理界面测试、信息泄露等），认证类（用户枚举、密码猜解、密码重置测试等），会话类（cookie测试、会话固定测试等），授权类（URL越权、路径遍历、业务逻辑、文件下载测试等）、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）、系统应用漏洞（溢出、0day漏洞等）等。

**源代码安全审计**：源代码安全审计以发现应用程序编码过程中造成的安全漏洞为目的， 通过源代码静态分析工具，对已有的代码进行扫描、分析，并对导致安全漏洞的错误代码进行定位和验证，然后提供补救建议。

**安全加固：**安全加固是针对系统脆弱性采取的一种有效的安全手段，可以提高系统抵御外来的入侵和蠕虫病毒袭击的能力，缩小影响范围，使被测系统可以长期保持在高度可信的状态。为了减小和避免安全加固操作对操作系统、数据库、应用系统和网络设备的影响，在加固方案设计和加固实施过程中会遵循标准性、规范性、可控性、整体性、最小影响等原则。

1. **项目预算及采购方式建议**

项目预算：本项目总预算合计10万元人民币，包括eMAS2.0平台和再·型-地震巨灾模型2.0两个项目，拟从“电子设备运转费”中调剂支出，不超电子设备运转费总预算。

采购方式建议：建议单一来源从北京启明星辰信息安全技术有限公司采购。北京启明星辰信息安全技术有限公司是集团信息安全外包服务项目的中标供应商，巨灾公司平台安全测评需按照集团统一安全管理要求，与集团安全测试标准和要求保持一致。依据公司采购管理办法 “必须保证原有采购项目一致性或者服务配套的要求，需要继续从原供应商处采购”。

供应商：启明星辰信息技术集团股份有限公司，供应商基本信息请见附件2。

1. **采购工作小组**

本项目采购工作小组成员共3人。包括：集团信息技术中心1人，巨灾公司信息技术部2人，监督人员1人，由综合管理部派遣。（详见附件3：采购工作小组名单）

1. **请示内容**

根据上述情况，信息安全测评服务项目拟立项并以单一来源的方式进行采购，采购总预算预计为10万元。

妥否，请批示。

信息技术部

2019.07.30