**关于启动金融科技实验室**

**安全专项研发的请示**

中心领导：

为积极落实提升关键金融基础设施安全能力的国家战略，金融科技实验室（以下简称实验室）已将交易安全作为重要的研究方向，并计划与外部领先机构合作，推进中心交易应用场景的安全专项研发，具体汇报如下。

1. **开展交易安全专项研发的意义**

作为我国重要的金融基础设施，中心应深刻洞察当前严峻的网络安全形势，加大网络安全方面的持续研发投入：**一是**HW攻防演练已暴露出中心安全监控与响应存在隐患，安全监控的覆盖面、准确性和及时性有待优化，防护效率有待提升。**二是**互联网交易是未来必然的发展趋势，相应的安全建设必须“走在前头”。伴随中心业务全球化以及互联网终端、终端开放等新业态的涌现，市场成员接入主体和方式更加多元化，核心业务系统风险集聚将进一步加剧。**三是**通用安全产品无法满足个性化应用安全需要。防火墙、入侵防御等通用安全序列产品的作用更在“治标”，而真正“治本”的方法在于深入“内建安全”，探索通过安全技术与中心技术框架的深度集成，从源头提升安全性。

1. **交易安全专项研发课题**

结合行业安全技术发展趋势和中心实际迫切需要解决的交易安全问题，评估确定首批研发课题（详见附件1）。

**一是中心统一终端和网关的“零信任”方案设计与改造，解决复杂网络环境下终端安全难以有效保障的问题。**中心核心交易系统基于边界的安全架构，经评估暂无法有效防护VPN 0-Day等恶意漏洞。HW已发现中心专线网服务器端口被互联网IP地址扫描的现象。开放互联网接入后，系统将暴露于更加复杂的网络环境中，攻击者通过XSS跨站脚本、CC攻击等攻击手段都可能入侵核心交易系统。采用零信任安全架构（Gartner预测2022年中80%的开放型数字业务将以此架构为基础进行网络访问）与中心统一终端和网关集成，可以提升交易系统安全性，构建细粒度的用户动态权限控制体系。

**二是开放客户端的安全服务，旨在建立与终端开放生态相适应的第三方组件安全管理能力。**统一终端基础框架是基于Web浏览器的桌面应用，继承Web浏览器的安全隐患。针对第三方的应用访问、调用后台服务、应用间通信的安全管控等问题，中心也尚未建立相应的授权管理体系。利用终端安全技术，可以提升终端组件间通讯安全，优化终端进程管理，从而推进开放终端框架安全改造。

**三是多源的威胁情报溯源，解决威胁流量“不能及时看到，无法及时响应”的问题。**攻击者组织化、国家化，系统接入主体多元化，导致攻击面扩张、攻击场景复杂化，对中心的安全监控与响应能力提出更高的要求。通过积累威胁情报，打造判别攻击行为的“武器库”，中心将更快速地识别并追溯异常攻击行为。

1. **下一步项目安排**

“零信任”设计改造、开放客户端安全课题由开发部牵头，运行部、一部、二部参与。威胁情报课题由运行部牵头，开发部参与（课题组成员及分工详见附件2）。上述研发课题并行推进，计划于2021年6月完成初步研发验证，2021年8月完成项目验收，验收通过即可启动用户无感的生产终端安全改造。

经调研安全领域头部供应商，奇安信集团、360企业安全集团、深信服科技与长亭科技四家基本满足中心现阶段安全研发需求。经与采管办确认，采用框架邀请招标向上述四家供应商采购相关技术开发和技术支持服务，三项子课题允许至多2家供应商承接。同时，建议与达成合作的外部技术供应商建立长期战略合作协议，并设立安全专项资源池。实验室可根据固定的人月单价，定向采购战略合作伙伴提供的安全技术服务。

统一终端和网关的“零信任”改造、开放客户端安全的集成改造部署等工作，由中汇公司负责实施。课题预算总额为630万元（详见下表1），可复用实验室现有硬件资源。

|  |  |  |
| --- | --- | --- |
| 类型 | 事项 | 预算 |
| 外部合作供应商研发费用 | 中心统一终端和网关的“零信任”方案设计与改造 | 100万元 |
| 开放客户端的安全服务 | 100万元 |
| 多源的威胁情报溯源 | 100万元 |
| 中汇公司研发费用 | 网关集成改造部署费用 | 100万元 |
| 终端集成改造部署费用 | 230万元 |

表1. 交易安全专项研发预算明细

以上妥否，请指示。

附件1. 金融科技实验室交易安全专项研发课题列表

附件2. 课题组成员及分工

附件3. 中心统一终端和网关“零信任”改造课题实施方案