附件 2

重要信息系统安全可控试点示范具体要求及项目资金申请报告编制要点

一、关于试点示范工程的总体要求（分不同领域）

（一）关于商业银行一体化信息安全风险感知体系试点示范的要求

按照信息安全等级保护的相关要求，建设信息安全风险感知体系。能够支持对银行重要信息系统中终端、网络、主机、应用和数据的业务、运维以及安全管理等操作行为进行主动感知，支持对相关多元化异构大数据进行预处理，对安全事件进行智能关联分析、集中展现和及时预警。支持银行网点终端统一管理，实现终端接入认证、访问控制、恶意代码防范、安全审计等功能。该体系分级分布式部署，具有可移植性、可扩展性，可并发会话数大于 1000 个，银行业务安全数据日处理能力大于 1000 万条，网点终端管理规模达到 20 万台以上。建立完善银行灾备系统建设、运行、维护、测评和应急处置的标准规范体系。制定第三方安全服务机构服务质量基本评价指标体系，包括第三方安全服务机构的制度体系评价指标、服务内容合规性评价指标、服务过程规范性评价指标、人员管理水平及稳定性评价指标、机构资质评价指标等，质量评价以量化分值方式呈现。

（二）关于商业银行开展电子银行和移动支付业务系统安全态势监控试点示范的要求

按照信息安全等级保护的相关要求，建设电子银行和移动支付业务系统安全态势监控体系。支持商业银行对电子银行系统（包括网上银行、手机银行及其门户网站等系统）、相关新型（增值）系统及其相关产品的安全态势进行监测预警，重点监控电子银行系统及其相关产品漏洞和入侵事件，对其存在的漏洞和重要信息安全事件进行预警，定期对其面临的信息安全形势作出分析研判；针对金融移动支付领域的各种主流操作系统应用，建立涵盖手机银行业务交易处理与关键流程安全性审核、客户端安全检测与防护措施验证、服务器端内控措施等多方面的安全检测与防护措施，并形成相应标准规范体系。提出手机银行从设计、开发、测试、部署、运维等不同阶段的安全性要求和实施要点，完善手机银行应用安全检测指引和相关安全设计规范。

（三）关于金融领域钓鱼网站和金融诈骗事件安全应急保障试点示范的要求

支持信息安全专业机构、商业银行、行业主管部门对电子银行系统联合建立针对钓鱼网站和金融诈骗事件的应急保障体系。研究建立信息安全专业机构、商业银行、执法部门联合处置、应急保障的协调机制。具体是:

信息安全专业机构应具有五年以上金融领域系统安全保障与咨询经验，能够1天内发现钓鱼网站，2天内将有关特征信息加入国家权威威胁库、各主流防病毒厂商病毒库及同步至CVE等国际公共威胁特征库并出具全面分析报告。

商业银行主要负责落实钓鱼网站与金融诈骗事件应急管理制度与预案，建设专用安全检查与通报平台，依托专业机构、联系行业主管部门和执法部门探索相关有效处置机制和管理规范。

行业主管部门应建立自动受理和快速处理的业务平台，组织取证材料，协调执法部门2天内关闭钓鱼网站，对于发生的金融诈骗事件在上报1至3天内，协调各家银行对涉事账户进行锁定、取证。

（四）关于云计算与大数据安全应用试点示范的要求

按照信息安全等级保护的相关要求，在金融、能源、交通、电子政务、电子商务和互联网服务领域，支持重点骨干企业，围绕主要业务应用，采用安全可控的技术和产品，建设完善云计算与大数据安全应用平台。平台应具有支持PB级动态安全域的安全存储、1000万以上并发业务访问，查询性能为秒级的能力，支持动态用户对大数据的限制性共享、数据所有者对存储在云端数据进行远程监控。具备对云计算与大数据应用平台进行漏洞扫描、配置基线检查、弱口令检测、版本检测和补丁管理等功能，可实现大数据去隐私

化处理和策略化数据抽取与集成、统一的策略管理、统一事件分析及多维度大数据审计，能够对用户访问敏感信息行为进行报警、阻断、跟踪和追溯，支持对虚拟化环境下各类设备的状态监测、数据取证等安全管理。研究制定云计算和大数据应用的安全管理机制、责任认定机制、数据保护和使用安全机制与规范。

（五）关于基于密级标识的涉密信息及载体管控试点示范的要求

按照分级保护管理的要求，在重点党政机构和涉密单位，开展电子文件密级标识管理系统、涉密计算机和涉密移动存储介质识别管理系统应用试点示范，部署管理平台，探索重要信息系统保密管理新方式。电子文件密级标识管理系统适用于各类常用电子文件，应符合定密管理规定，能够生成显性和隐性密级标识，支持涉密电子信息流转、读写、打印管控，电子文件密级标识具备防篡改保护。涉密计算机和涉密移动存储介质识别管理系统应采用 RFID 技术，具备无线识别功能，使用符合相关管理规定和规范的编码方式，支持涉密计算机、涉密优盘、涉密光盘、涉密打印机等涉密载体、涉密设备的全生命周期管理，对违规带出等行为进行实时报警并记录日志。

（六）关于安全邮箱试点示范的要求

支持互联网企业或相关专业机构与国家信息安全权威机构合作开展电子邮箱安全保密试点示范，基于国家公共信息基础设施或国内大型 IT 企业公共云设施平台，综合利用基于标识技术的国家商用密码 SM9 专用算法加密与邮箱平台内核防护技术，结合国家信息安全权威机构定点监测，建设安全邮箱服务平台，形成电子邮箱防泄密、反窃密综合保障能力，面向有工作信息保护需求的商业机构、政务部门、团体组织和个人提供可靠的安全加密邮件与智能终端电子邮件消息加密推送等商业化运营服务，研究电子邮件安全整体技术方案与服务规范。

（七）工业控制信息安全领域示范应用的要求

面向电力电网、轨道交通等多级的生产控制环境，形成广域安全生产监测系统。对各所属生产企业重要设备运行数据进行采集、分析和故障诊断，以工业控制核心系统安全运行为目标，实现基于公网或专网的数据安全传输、移动设备安全接入、行为综合审计等安全功能。

面向石油石化等流程工业的生产控制环境，在集散控制系统中进行防火墙、入侵检测系统、入侵防御系统、安全审计系统、安全数据交换系统等系列安全可控产品的试点应用，验证现有信息安全产品对 SCADA 软件、现场总线、嵌入式控制软件的技术影响，形成工业控制系统有针对性的有效安全防护策略，并开展相应的工业控制系统信息安全标准

体系及等级保护标准研究制定与验证。

面向先进制造的生产控制环境，采用安全可控的技术和产品，开展试点示范应用，协同设计与过程控制的示范应不少于3个安全域、100个用户终端，加工环节的应用示范应不少于3种类型、10台联网生产制造设备、2种类型的分布式数字控制（DNC）系统。

二、关于试点示范工程资金申请报告的编制要点

（一） 项目简介

简述试点项目背景、承担单位情况，以及项目目标、规模内容、建设期、总投资和资金来源，经济与社会效益等。

（二）项目建设的必要性和需求分析

1、项目建设的背景和依据、以及要实现的业务目标和信息化系统建设目标。

2、现有信息系统装备和信息化应用状况，以及存在的信息安全问题。

3、项目示范的主要内容、目的，以及对本部门、本地区或本行业的带动作用。

4、项目的预期效果。

（三）建设方案

1、建设目标与主要建设内容：描述项目建设目标，尽可能提出可量化、可考核的目标。简述各项建设内容和建设规模。

2、拟使用验证的自主信息安全技术标准和管理规范。

3、自主信息安全装备选型的原则、参考清单，以及使用验证自主信息化装备的工作思路。

（四）投资估算和资金筹措

总投资、资金来源与落实情况：明确项目投资的资金来源和落实情况。须附地方投资和项目建设单位自筹资金的意向承诺函或资金证明。