国家发展和改革委员会办公厅文件

发改办高技〔2013〕1965号

国家发展改革委办公厅关于组织实施2013年国家信息安全专项有关事项的通知

工业和信息化部、公安部、安全部、质检总局、中科院、国家保密局、国家密码局办公厅（室），各省、自治区、直辖市及计划单列市、新疆生产建设兵团发展改革委，相关中央直属企业：

为了贯彻落实《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）的工作部署，针对金融、云计算与大数据、信息系统保密管理、工业控制等领域面临的信息安全实际需要，国家发展改革委决定继续组织国家信息安全专项。现将有关事项通知如下：

一、专项重点支持领域

（一）信息安全产品产业化

产品自身应具有较高的安全性，不低于目前 GB/T 20281-2006、GB/T 20275-2006、GB/T 18336-2008 等国家标准中 3 级的相关要求。

1、金融信息安全领域

（1）金融领域智能入侵检测产品。适用于金融机构电子银行等应用业务系统，支持 IPv4/IPv6 环境，具有双向数据检测、历史数据关联分析、网络报警数据筛选过滤、反馈测试、自学习和自定义检测规则、多维度展现，以及攻击影响分级等功能，吞吐量不低于 20Gbps，基于国内外主流特征库检测的漏报率低于 10%、误报率低于 5%。

（2）高级可持续威胁（APT）安全监测产品。适用于金融机构的业务网络和应用系统，支持 IPv4/IPv6 环境，具有规模化虚拟机或沙箱执行等动态检测技术的威胁感知功能，具备对各类设备网络文件传输异常行为、漏洞利用行为、未知木马、隐蔽信道传输等多样性、组合性和持续性攻击的检测能力，支持 1000 个以上的并发检测能力，基于国内外主流特征库检测的漏报率低于 5%、误报率低于 10%。

（3）面向电子银行的 Web 漏洞扫描产品。适用于金融机构电子银行业务系统，具备开放式 Web 应用程序安全项目（OWASP）通用漏洞的高启发、高强度、交互式检测能力，具有漏洞验证、基于电子银行系统业务流程的流量录制重放式的逻辑漏洞分析等功能，

基于国内外主流漏洞特征库扫描的漏报率低于5%、误报率低于10%。

(4)金融领域应用软件源代码安全检查产品。适用于金融机构各类业务应用系统,具备适用于金融领域特点、可更新和自定义的安全扫描规则库,可定制扫描策略,在Linux、Aix、Windows、Android、iOS等环境下,具有对Java、C/C++、C#、JSP、COBOL、VB、Ruby等主流编程语言和.NET、Eclipse、Matlab等集成软件工具开发的应用系统进行源代码扫描的功能,对源代码潜在问题分析给出分级别建议,每小时扫描百万行以上代码,基于国内外主流软件源代码漏洞特征库检测的误报率低于30%、漏报率低于35%。

2、云计算与大数据信息安全领域

(1)高性能异常流量检测和清洗产品。支持IPv4/IPv6环境,适用于云计算和大数据的应用,具备流量牵引和回注、网络层和应用层攻击检测与清洗等功能,支持地址区间的IP保护,可实现对100万个以上IP地址的异常攻击流量清洗,启用全部检测和清洗功能后,设备整体吞吐量达到100Gbps以上。

(2)云操作系统安全加固和虚拟机安全管理产品。支持IPv4/IPv6环境,支持虚拟化认证授权、访问控制和安全审计,具备虚拟机逃逸监控、实时操作监测与控制、防恶意软件加载和安全隔离等功能,具备1万台以上安全可控轻量级虚拟机的安全管理能力。

(3)高速固态盘阵安全存储产品。支持IPv4/IPv6环境,具备

双控及冗余保护机制，具有缓存镜像、掉电保护、采用国家密码局规定算法的数据加密等功能，支持原生命令队列（NCQ）技术及多种主流接口协议，单盘持续读写性能不低于200MB/s，容量大于512GB，每秒输入输出次数（IOPS）大于12,000，单阵列支持500块以上单盘扩展，响应时间小于800μs，非加密通道IOPS大于220,000，加密吞吐量大于1Gb/s。

（4）大数据平台安全管理产品。支持IPv4/IPv6环境，具有对不少于3种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、全文检索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，关键安全策略同时支持结构化与非结构化数据的管理，支持1000万以上并发业务访问。

3、信息安全分级保护领域

（1）网络保密检查和失泄密核查取证产品。适用于涉密网和普通业务网络，支持各类主流操作系统，具备对各种网络失密泄密事件证据保全、提取和分析的功能，支持只读方式、多种硬盘接口、DD或AFF等多种镜像格式，支持已删除文件、注册表、分区的恢复，具有自定义策略取证、关键词搜索、2000万个以上文件并行搜索、加密文件快速检测的能力，对带有密级标志的图形、版式等类型文件识别率大于95%。

（2）特殊木马检查产品。适用于涉密网和普通业务网络，支

持各类主流操作系统，具有已知木马和未知特殊木马检测的能力，具备木马样本及其配置信息的提取、特征归类检测等功能，能够定期进行升级，已知木马检测准确率为100%，未知特殊木马检测准确率大于70%。

（3）涉密信息系统安全保密风险评估软件产品。符合涉密信息系统分级保护相关国家保密标准，具备合规性检测、漏洞扫描等功能，以自动检测为主、人工判定为辅，评估内容覆盖涉密信息系统安全保密风险评估全部项目，评估结论准确可靠，能够自动生成评估报告。

4、工业控制信息安全领域

（1）面向现场设备环境的边界安全专用网关产品。支持IPv4/IPv6及工业以太网，适用于集散控制系统（DCS）、数据采集与监视控制系统（SCADA）、现场总线等现场环境，具备5种以上工业控制专有协议以及多种状态或指令主流格式数据的检查、过滤、交换、阻断等功能，数据传输可靠性达到100%，可保护节点数不少于500点，设备吞吐量达到线速运行水平，延时小于100ms。

（2）面向集散控制系统（DCS）的异常监测产品。适用于电厂、石油、化工、供热、供水等工艺流程，具有对工业控制系统的DCS工程师站组态变更、DCS操作站数据与操控指令变更，以及各种主流现场总线访问、负载变更、通信行为、异常流量等安全监测能力，具备过程状态参数、控制信号的阈值检查与报警功能。

（3）安全采集远程终端单元（RTU）产品。支持工业以太网协

议，适用于-40℃～+70℃温度环境，电磁兼容性（EMC）不低于4级，具有内置安全模块，实现数据采集与监视控制系统（SCADA）软件端到端的信源加密，具备基于数字证书的安全认证功能，支持基于国家密码局规定算法的数据加密，加密速率不小于20Mb/s。

（4）工业应用软件漏洞扫描产品。适用于石油化工、先进制造领域，具有对符合IEC61131-3标准的控制系统上位机（SCADA/HMI）软件、DCS控制器嵌入式软件以及各种主流现场总线离线漏洞扫描能力，具有对数字化设计制造软件平台（如产品数据管理PDM、专用数控机床通信软件eXtremeDNC、高级设计系统ADS等）漏洞扫描能力，具备检测与发现软件安全漏洞、评估漏洞安全风险、可视化展示、漏洞修复建议等功能，漏洞检测率达到90%以上。

（二）重要信息系统安全可控试点示范

1、金融信息安全试点示范。

支持商业银行开展一体化信息安全风险感知体系试点示范，按照信息安全等级保护相关要求，建立银行系统整体信息安全风险感知预警、网点集中管控的防护体系，完善灾备能力检测、第三方安全服务质量评价等管理规范。

支持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，按照信息安全等级保护相关要求，构建银行新型增值业务应用的安全管理机制，并形成相应标准规范体系。

支持商业银行、信息安全专业机构、行业主管部门对电子银行系统联合开展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，探索银行、机构和政府部门合作的新模式，建立联合处置、及时有效的应急保障机制。

2、云计算与大数据安全应用试点示范

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，开展云计算和大数据安全应用试点示范，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。

3、信息系统保密管理试点示范

在国家重点党政机构和涉密单位，按照信息安全等级保护相关要求，开展基于密级标识的涉密信息及载体管控试点示范，部署电子文件密级标识管理、涉密计算机和涉密移动存储介质识别管理等系统，探索重要信息系统保密管理新方式。

支持商业机构、专业机构开展电子邮箱安全保密试点示范，采用国家密码局规定算法，以及相关信息安全防护技术，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，探索安全加密邮件与智能终端电子邮件消息加密推送等新服务模式。

4、工业控制信息安全领域示范

在电力电网、石油石化、先进制造、轨道交通领域，支持大型重点骨干企业，按照信息安全等级保护相关要求，建设完善安全可控的工业控制系统。建立以杜绝重大灾难性事件为底线的工业控制系统综合安全防护体系，建立完善工业控制信息安全技术与管理

的机制和规范。

二、申报要求

（一）请项目主管部门根据投资体制改革精神和《国家高技术产业发展项目管理暂行办法》的有关规定，结合本单位、本地区实际情况，认真做好项目组织和备案工作，组织编写项目资金申请报告并协调落实项目建设资金、环境影响评价、节能评估等相关建设条件，同时汇总相关申请材料并报我委。

（二）通过国务院有关部门及中央直属企业申报的项目，项目单位应与有关部门和中央直属企业有财务隶属关系。其他项目应按照属地管理原则，通过项目单位所在地的省级发展和改革委员会申报。

（三）项目主管部门应对报送的材料，如资金申请报告、银行贷款承诺、自有资金证明、各类许可资质等，进行认真核实，并负责对其真实性予以确认。

（四）项目纸质申报材料包括：项目资金申请报告（达到可行性研究报告深度）、项目简表和项目汇总表，上述材料一式两份。项目简表、项目汇总表、项目备案文件、自有资金证明、投资及信贷承诺等所有附件要与项目资金申请报告一并装订（项目简表和汇总表应订装在报告正文前）。各项目材料一经提供不予退还，请做好备份。资金申请报告的具体编制要求详见附件1、2。

（五）项目材料的具体报送时间、地点和相关要求将在今年9月下旬在国家发展改革委高技术司网站（网址 http://gjss.ndrc.

gov.cn)信息化栏目下另行通知。

(六)信息安全产品产业化项目的承担单位原则上应为企业法人。申报项目应具备以下条件:(1)按规定在当地政府备案;(2)已落实项目建设资金;(3)采用的科技成果应具有自主知识产权;(4)项目申报单位必须具有较强的技术开发和项目实施能力,具备较好的资信等级,资产负债率在合理范围内;(5)项目答辩时各单位应已有相关产品。

(七)重要信息系统安全可控试点示范项目的承担单位应为企业法人或事业法人(不包含高校和科研机构),项目的具体要求及项目资金申请报告的编制要点详见附件2。

(八)本次信息安全专项分两阶段开展。第一阶段受理金融信息安全、云计算与大数据安全、信息系统保密管理项目的申报,截止时间为2013年10月15日。第二阶段受理工业控制信息安全项目申报,截止时间为2014年7月15日。我委对项目进行初步评审后,将组织现场答辩。其中,专项拟支持的产品将全部委托第三方检测机构进行公开测试,有关具体项目答辩和测试名单、时间和地点,以及公开测试的时间将另行通知。

附件:1、信息安全产品产业化项目资金申请报告编制要点

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

3、信息安全项目及承担单位基本情况简表

4、信息安全项目汇总表

（此页无正文）

国家发展改革委办公厅

2013年8月12日

附件 1

信息安全产品产业化项目资金申请报告编制要点

一、项目简介

简要介绍项目基本情况、建设目标、建设内容、总投资等内容。

二、项目的意义和必要性

国内外现状和技术发展趋势，项目的需求和市场分析，产业关联度分析，项目建设的必要性，以及与信息安全专项总体思路、原则、目标等相关联情况。

三、项目的产业化基础

项目单位技术创新、生产和销售的能力，以及相关领域研发基础和研发队伍情况；项目技术成果来源及知识产权情况，已完成的研究开发工作及中试情况和鉴定年限，技术或工艺特点以及与现有技术或工艺比较所具有的优势，该重大关键技术的突破对行业技术进步的重要意义和作用。

四、建设方案

项目的产能规模、建设的主要内容、采用的工艺技术路线与技术特点、设备选型及主要技术经济指标、建设地点、

项目实施与进度计划安排、建设期的组织管理等。

五、环境保护、资源综合利用、节能措施

节能、降耗、环保、安全、原材料供应及外部配套条件落实情况等。

六、项目法人基本情况

包括所有制性质、主营业务、近三年来的销售收入、利润、税金、固定资产、资产负债率、银行信用等级、项目负责人基本情况及主要股东的概况。

七、投资

项目总投资规模，投资使用方案和资金筹措方案；申请国家补贴资金的主要理由和政策依据。

八、项目财务分析、经济分析及主要指标

内部收益率、投资利润率、投资回收期、贷款偿还期等指标的计算和评估，项目风险分析与控制，经济效益和社会效益分析。

九、资金申请报告附件

1、银行承贷证明(省级分行以上)文件。

2、项目法人近三年的经营状况（包括损益表、资产负债

表、现金流量表）和项目法人自筹资金保证落实文件。

3、地方、部门配套资金及其它资金来源证明文件。

4、前期科研成果证明材料(成果鉴定、权威机构认证或出具技术检测报告、专利证书等)；前期科研成果的成熟度，应能够满足产业化试验或产业化示范的要求。

5、环保部门出具的环境影响评价文件的审批意见。

6、土地、重要原材料以及其它所需证明材料。

7、企业投资项目的核准或备案的批准文件（在有效期内且未满两年）；已开工项目需提供投资完成、工程进度以及生产情况证明材料。

8、项目招标内容（适用于申请国家补贴资金500万元及以上的投资项目）。

9、项目单位对项目资金申请报告内容和附属文件真实性负责的声明。

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。

附件3

信息安全项目及承担单位基本情况简表

单位：万元

项目名称		项目负责人		固定电话	
				手　　机	
				电子邮件地址	
项目单位名称		项目联系人		固定电话	
				手　　机	
				电子邮件地址	
项目主持部门		项目所属领域 （精确到每个领域子项）			
项目单位地址		建设地点			

项目投资情况		单位法定代表人		企业情况	2010年	2011年	2012年
项目总投资		法定代表人电话		企业总资产			
固定资产投资		企业注册登记类型		固定资产净值			
铺底流动资金		银行信用等级		资产负债率			
拟申请银行贷款		职工人数		销售收入			
自筹资金		技术人员数		利税			
		有无银行贷款承诺函		出口创汇			

项目建设必要性：

项目主要建设内容及目标：　（产业化类项目应包含项目建成后每年产品生产数量）

填表说明：

1、本表由企业填报，主持部门认真审核后打印填报

2、项目总投资＝自有资金＋银行贷款＋其他资金　（即申请国家补助资金暂不列入资金来源部分）

3、项目所属领域，请按照信息安全专项重点所列范围填写（参见通知正文。务必精确到每个领域子项）

4、联系人：国家发展和改革委员会高技术产业司　刘　勇　　张　岩　　010-68501562　15811128359　Email：xxhc@ndrc.gov.cn

附件4

信息安全项目汇总表

单位：万元

序号	主持部门	企业名称	项目名称	所属领域	总投资	资金来源		申请国家补助资金	项目负责人及联系方式	项目联系人及联系方式	起止年限	项目建设内容（产业化类项目应包含项目建成后每年产品生产数量）
						企业自筹	银行贷款					
1												
2												
3												
4												

填表说明：

1. 项目总投资＝企业自筹＋银行贷款 （即申请国家补助资金暂不列入资金来源部分）
2. 项目所属领域，请按照信息安全专项重点所列范围填写（参见通知正文。务必精确到每个领域子项）
3. 在填写过程中，请不要合并或者拆分此表单元格，请不要打乱表头次序。
4. 表格中所填数字均不包含小数部份