

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

发改办高技[2013]1965 号

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 800 μ s，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