**《安全保障专项行动计划》**

**一、指导思想**

深入贯彻落实国务院《关于加快培育和发展战略性新兴产业的决定》和《关于推进物联网有序健康发展的指导意见》，按照“创新发展、应用牵引、评建结合、安全可控”的原则，加快推进核心安全技术、专业安全产品研发，推进物联网信息安全保障体系建设，建立健全物联网信息安全的监督、检查和安全评估机制，提高我国物联网信息安全保障能力。

**二、总体目标**

到2015年，在物联网核心安全技术、专用安全产品的研发方面取得重大突破，物联网系统安全标准化工作得到强化，在物联网安全领域形成一批自主研制的国家标准和行业标准；进一步完善涉及物联网的信息安全等级保护制度，初步建立健全物联网安全测评、风险评估、安全防范、应急处置等机制，增强物联网信息采集、传输、处理、应用等各环节的安全保障能力。

**三、重点任务**

**（一）推进物联网关键安全技术研发与产业化。**鼓励国家工程中心、实验室等科研资源的开放和共享，推进技术成果转化，引导信息安全企业与物联网技术研发与应用企业、科研机构、高校合作，联合开展信息安全技术和产品研发，促进物联网安全技术和产品的研发与产业化。

**（二）加强物联网安全标准实施工作。**围绕国家物联网安全保障工作实际需求，跟踪技术和标准化发展动态，推动国家标准和行业规范的制定。加强物联网系统及其安全标准化战略与基础理论研究，强化标准的自主研制、验证和推广实施，全面提升物联网安全标准的质量和实施成效。

**（三）建设物联网信息安全技术检测评估平台。**在已有国家级信息安全检测机构基础上，整合国内信息安全领域优势资源，完善物联网安全技术检测评估平台，依托现有基础，围绕物联网系统解决方案、核心设备与运营服务等，完善物联网系统安全评估机制，加强物联网安全产品测评，满足物联网系统的数据保护和安全风险管理需求。

**（四）建立健全物联网系统全生命周期的安全保障体系。**建立健全物联网信息安全等级保护制度，开展物联网系统安全等级测评与检查、评估工作。在物联网系统设计研发阶段，对设计方案进行安全验证与风险评估；在物联网项目竣工验收阶段，对系统的安全防护能力进行测试和评估；在物联网系统运营阶段，适时开展安全检查工作，查找突出问题和薄弱环节，评估安全防护水平。同时，建立相关信息采集交换平台与信息共享分析机制，在物联网工程的全生命周期提供安全监测和预警服务。

**（五）开展物联网应用安全风险管理建设试点。**从物联网信息安全监管、可信身份认证和安全控制、网络安全防护、隐私保护等方面，开展支撑物联网信息安全保障体系建设的试点工作。针对国家公共安全与基础设施等重点领域的物联网应用，加强对系统解决方案、核心设备与运营服务的风险评估，研究制定“可发现、可防御、可替换”的物联网安全保障长效机制。

**四、分工与进度**

具体分工与进度如下表所示：

**重点任务分工与进度表**

|  |  |  |  |
| --- | --- | --- | --- |
| **任务** | **专项行动** | **负责部门** | **时间进度** |
| （一）推进关键安全技术研发与产业化 | 1、推进关键安全技术研发与产业化 | 科技部、工业和信息化部、发展改革委、公安部 | 2013年底完成关键技术立项，2015年实现30项科技成果转化 |
| （二）加强物联网安全标准实施工作 | 2、加强物联网安全标准实施工作 | 国家标准委、工业和信息化部、公安部 | 2013年完成第一批专家团队遴选和组建工作，2014年启动安全标准自主研制、验证和推广实施机制的研究工作 |
| （三）建设物联网信息安全技术检测评估平台 | 3、建设物联网信息安全技术检测评估平台 | 工业和信息化部、发展改革委、公安部、总参信息化部、国家密码管理局 | 2013年完成物联网信息安全技术研究并验证、测试平台建设方案论证，2014年底前支持2-3家国家级科研机构并以产学研用联合的方式开展平台建设，2015年底前完成平台基础环境建设并全面开展服务 |
| （四）建立健全物联网系统全生命周期的安全保障体系 | 4、建立健全物联网系统全生命周期的安全保障体系 | 公安部、工业和信息化部、总参信息化部、国家保密局、发展改革委 | 2013年开展物联网信息安全等级保护制度的研究，2014年完成预警与态势通报机制、信息共享与分析机制建立与基础环境建设，2015年全面推广安全保障体系 |
| （五）开展物联网应用安全风险管理建设试点 | 5、开展物联网应用安全风险管理建设试点 | 工业和信息化部、公安部、发展改革委、总参信息化部 | 2013年开展信息安全调研，形成物联网风险评估报告，2014年形成物联网应用全生命周期安全风险管理试点建设方案并分两批选择重点领域开展试点工作，2015年底形成物联网应用全生命周期管理规范并向全国推广 |

**五、保障措施**

**（一）加强组织协调。**建立和完善协同工作机制，加强部门合作与信息共享，协调社会资源参与物联网安全保障工作，建立重要网络基础设施预警机制，研究应急响应预案和应急措施。建立物联网应用建设相关主体沟通协调机制，研发机构、生产企业、行业用户、主管单位共同参与，构建安全技术的研究、转化、效果评估、需求反馈的闭环系统。

**（二）重视资金投入。**重视物联网项目中用于信息安全的资金投入。物联网项目主管部门在审批物联网项目时，应增加对信息安全建设预算科目的审查，确保一定比例的建设资金用于同步规划和设计安全防护方案，保障物联网信息安全保障体系与物联网建设相适应。在相关的国家科研项目中，增加对安全防御技术和产品与安全测评工具研发的支持力度。

**（三）加强国际交流。**积极开展国际交流，鼓励技术应用企业、研发企业、科研机构、信息安全服务机构等单位开展国际技术合作，引进国际先进的信息安全理论、技术和管理经验，并通过消化吸收努力提高创新能力和竞争力。吸引国际技术、人才资源，提高信息安全研发、生产能力，不断提升安全保障能力。

**（四）优化发展环境。**通过开展形式多样的物联网知识和技能普及活动，推动建立并完善多层次的物联网系统人才培养和服务体系，营造有利于复合型、领军型高端人才脱颖而出的发展环境。利用多种途径，通过实际案例，加强宣传、教育和培训，提高安全意识和技能，增强风险意识、责任意识，切实加强物联网系统信息安全认识，提高安全管理水平。