附件2

《物联网基础安全标准体系建设指南》

（征求意见稿）编制说明

为进一步加强物联网基础安全管理，按照《中华人民共和国网络安全法》等相关法律规定，工业和信息化部组织制定了《物联网基础安全标准体系建设指南》（以下简称《建设指南》），加强物联网安全标准的顶层设计和方向引领，指导物联网安全工作规范有序开展。现就有关编制情况说明如下：

1. 编制背景和必要性
2. 当前面临的形势和挑战

随着5G、人工智能、大数据等新一代信息技术发展，促进了物联网应用普及，催生了众多跨行业、跨领域的新业态，人类社会加速迈入万物互联时代。与传统互联网相比，物联网“无缝连接、全面感知、智能处理、虚实交织”的特点突出，行业安全需求多样。随着5G网络覆盖日益完善，物联网产品应用日益丰富，行业渗透日益加深，物联网关键基础环节的一些安全风险将更为突出，集中体现在：物联网卡违规挪用时有发生；海量物联网终端安全能力较为薄弱，一旦被攻击控制，风险极易从单点扩散至全网；物联网网关和平台在安全防护、数据保护等方面亟需加强。因此，聚焦物联网终端、网关、平台等关键环节，加快构建物联网基础安全保障体系，促进物联网安全健康发展尤为重要。

1. 当前存在的主要问题

一是物联网安全标准整体缺乏规划，各项标准较为分散，缺乏统一的物联网安全标准体系。二是现有标准内容相对笼统，对于技术细节界定较少或无具体要求，没有明确安全技术基线，难以有效指导各类行业应用落实安全要求。三是部分物联网标准制定年份较早，随着技术进步，一些内容已与现有产业发展不符，不再适合物联网发展需要。

1. 标准体系建设意义

紧扣我部职责定位，建立物联网基础安全标准体系，推动制定完善物联网终端、网关、平台等关键环节技术标准，有利于完善我国物联网的标准体系，有利于提升物联网行业整体安全水平，有利于促进物联网安全发展。

1. 《建设指南》编制过程

2020年2月，在工业和信息化部组织下，成立了由中国信息通信研究院牵头，运营商、设备商、互联网企业、安全企业等产业各界广泛参与的《建设指南》起草组，启动了文件编制工作。起草组深入分析了当前物联网行业所面临的形势，梳理物联网安全标准的现状和需求，初步形成了物联网基础安全标准体系框架。

2020年7月，起草组召开专题研讨会，与会专家对《建设指南》的体系框架、层级、内容等方面提出了多项建设性修改建议。起草组充分吸收与会专家意见，对《建设指南》进行了修改完善。

2020年9月，起草组就《建设指南》向中国电信、中国移动、中国联通、华为、阿里云、腾讯、小米、奇安信、中国信息通信研究院和中国通信标准化协会等单位征集意见，共收到意见47条。起草组对各单位的意见进行认真研究和吸收采纳，并对《建设指南》进一步修改完善。

1. 《建设指南》主要内容

《建设指南》主要包括建设思路及目标、建设内容、组织实施三个部分。

一是建设思路及目标。明确了物联网基础安全标准体系建设的总体思路、基本原则、建设目标。

二是建设内容。提出了物联网基础安全标准体系框架、物联网基础安全重点标准化领域及方向，包括总体安全要求、终端安全、网关安全、平台安全、安全管理五大类标准。

总体安全要求包括物联网基础安全术语定义、架构模型、安全场景、安全集成、安全分级及应用等方面标准，可为各类标准制定提供基础性支撑。终端安全标准从卡安全、模组安全、通信芯片安全、终端设备通用安全、行业终端安全、终端测试评估等方面对终端安全技术要求进行规范。网关安全标准包括物联网网关设备安全、网关数据交换与处理安全、网关通信与接口安全、网关物理环境安全、网关组件安全、网关测试评估等内容。物联网平台安全标准包括平台通用安全、平台业务系统安全、平台交互安全、平台测试评估等，有效指导平台的安全管理和维护。安全管理主要用于指导行业落实安全管理要求，包括安全信息协同、管理与维护安全、证书管理等标准。

三是组织实施。通过加快标准研制、实施动态更新、深化标准应用、加强交流合作等四方面工作，指导物联网基础安全标准化工作规范有序开展。