

国家标准

# 智慧城市建设信息安全保障指南

编制说明

标准编制组

二〇一七年五月

# 1 标准工作概况

## 1.1 前言

建设智慧城市，是我国抓住新一代网络技术、新一代智能制造产业、新一代服务业和城市化发展的机遇，破解城市发展难题，事关经济转型升级、社会管理创新和人民生活品质提升的一项系统性、创新性工作。智慧城市作为一项复杂的大型系统工程，其安全问题尤显重要。围绕智慧城市信息系统的规划、设计、建设、运行、使用和维护，需要借助技术措施和管理措施两方面的控制，在统一安全策略的指导下，安全事件的事先预防、事发处理、事后恢复的相互配合，构建一个完整的保障体系。迫切需要依据有关信息安全技术与管理标准，对信息网络和信息系统及其存储、传输、处理的信息的保密性、完整性、可用性和不可抵赖性等安全属性进行评价，降低信息资产被泄露、被更改、被破坏及非预期使用的可能性。

标准参考了 GB/T 33356-2016《新型智慧城市评价指标》，GB/T 31495.2-2015《信息安全技术 信息安全保障指标体系及评价方法 第2部分：指标体系》、智慧城市安全体系框架、系统虚拟化安全技术要求、大数据基础平台安全要求等，并且通过在浙江省进行试点，具有一定的试用性和有效性，后期会扩大试点城市及不同的行业应用，增强通用性；标准中提到了会对关键信息基础设施是否进行风险评估、等级保护及 4A 认证的进行评价考察。

## 1.2 标准的作用

本项目研究编制目的是贯彻国务院《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》等政策文件精神，遵循“综合防范，保障安全”的基本原则，确保智慧城市建设运营中网络应用市场主体各方面的权益、运营秩序和信息安全，增强抵御风险和自主可控的能力，指导智慧城市建设项目信息安全保障体系规范，对智慧城市建设项目信息安全保障体系架构所涉及的不同阶段和其对象等提出相关要求。

## 1.3 任务来源

智慧城市是一项复杂的大型系统工程，其安全问题尤显重要：在未来网络时代未根本解决好安全问题的情况下，系统的信息感知层、接入与传送层、应用层与终端层、智能/智慧处理及协同平台层等诸多层面存在不安全因素；不可或缺的云化支持与社会管理环境等也带来诸多突发性不安全因素。这些不安全因素可能会影响整个城市，导致工厂停产、商店停业、电气中断、交通瘫痪、水源切断等，使城市陷入一片混乱，造成极严重后果，因此必须倍加重视与小心务实应对。

为推进在我国智慧城市建设，指导基于物联感知、海量数据的智慧城市信息安全保障工作，特制定本指导性技术文件。2013年9月2日，全国信息安全标准化技术委员会秘书处将“智慧城市建设信息安全保障指南研究”作为研究类项目予以正式立项（信安秘字[2013]027号《关于通报全国信息安全标准化技术委员会2013年信息安全标准项目的通知》）。

## 1.4 工作过程

2013年9月，在WG1国家标准工作组的领导下，按照国家标准制修订管理要求成立标准研究编制工作组。工作组由省经信委信息安全协调处指导，省经济信息中心牵头，省电子产品检验所、省标准化研究院、浙江传媒学院等单位共同参与。

2013年10月，成立标准编制工作组并召开第一次工作组会议，正式启动《智慧城市建设信息安全保障指南研究》国家标准的研究工作。会议介绍标准研究背景、讨论标准研究初步思路、初步讨论落实工作组成员分工。浙江省经济信息中心负责整个项目研究的总体工作及主要研究任务。浙江省标准化研究院负责标准研究相关咨询与资料收集等任务。浙江省电子产品检验所、浙江传媒学院协助配合智慧城市信息安全保障中的技术研究任务。

2013年10月至11月，工作组根据任务分工收集国内外智慧城市建设信息安全建设标准和其他相关材料，整理出相关材料清单。根据整理收集资料，搭建标准框架。

2013年12月，由浙江省经信委信息安全协调处指导，于12月13日组织会议，增强扩充原标准研究组为标准制定课题组。由浙江省经济信息中心(省信安标委秘书处)作为第一承担单位。在研究组参与单位名单基础上，为进一步提高项目研究与标准制定的质量，特别是在涉及智慧信息技术等领域的深入研究，增加省内外相关领域龙头单位参与，扩充增强后的标准编制课题组承担各单位分工如下：

浙江省经济信息中心负责整个项目研究编制的总体工作及智慧城市信息安全保障技术和管理体系主要研究任务；中国管理

科学研究院提供信息安全标准研究与制定，以及智慧技术研究方面的丰富经验指导，西南科技大学负责智慧城市信息安全产品检测技术研究任务；中电长城网际系统应用有限公司主要负责物联网、智能感知终端设备等智慧技术安全研究等任务；华三通信技术有限公司主要负责大数据、云平台等智慧技术安全保障研究；浙江科技学院主要负责智能建筑电气、深度互联等智慧技术安全保障研究；省标准化研究院主要负责智慧城市标准研究相关咨询与资料收集等任务；杭州奕锐电子有限公司主要负责智慧城市建设数据存储与传输加密研究；省卫生信息中心作为牵头单位，负责典型试点领域之智慧健康（医疗）信息安全保障研究；浙江传媒学院主要负责多媒体、虚拟全景、体感互动等智慧技术安全保障研究；省交通集团作为牵头单位，负责典型试点领域之智慧交通信息安全保障研究。

2013年12月至2014年2月 标准研究编制组根据任务分工，调研国内外智慧城市信息安全保障及相关标准化现状，明确智慧城市建设项目信息安全保障体系规范，研究智慧城市建设项目信息安全保障体系架构及相关要求，确定并编写了智慧城市建设信息安全保障指南标准制定研究报告总体框架。

2014年2月19日在参加了全国信息安全标准化技术委员会秘书处组织的2013年第二批信息安全国家标准项目任务书评审会议，专家组对前期工作提出了宝贵的意见。根据专家意见，为进一步提高项目研究的质量，特别是在面向全国智慧城市建设信息安全保障的广泛性和权威性方面考虑，增加中国电子技术标准化研究院、中国信息安全测评中心两家国家级单位参与项目规

划与组织，参与标准文本的编写。

2014.3月至6月，标准研究编制组根据任务分工，对各自承担部分的内容进行研究，形成标准初稿。并以多种形式征求专家和相关单位意见，形成标准草案。编写标准草案编制说明。

2014.7月中旬，国家信安标委秘书处组织全国信息安全标准领域专家，对“信息安全技术 智慧城市建设信息安全保障指南”编制工作进行了现场检查。检查组听取了标准研制工作组关于标准编制情况的汇报，对标准的框架及内容进行了质询和讨论。检查组充分肯定了标准编制组织工作，对智慧城市信息安全保障指南提出了意见和建议。

根据专家组提出的意见和建议，“信息安全技术 智慧城市建设信息安全保障指南”标准研究与编制项目经多次修改完善，并在2014年9月和11月分别在江西南昌和浙江杭州两次通过国家信息中心组织的部分省市经济信息中心会议，进行研讨征求意见。

信安标委秘书处所在单位积极支持信安标委工作，2014年设立自主研究课题“新一代智慧信息化安全保障体系研究”，开展智慧信息技术之云计算技术多租户数据隔离、虚拟边界防护以及无线技术等安全保障体系研究，为后续信息安全标准工作打下坚实基础。

“信息安全技术 智慧城市建设信息安全保障指南”标准研究项目经多次修改完善并征求意见后，于2015年1月底向国家信安标委提交了《智慧城市建设信息安全保障指南研究报告》，并听取专家评审组意见，研究报告内容和形式得到国家信安标委

专家评审组的肯定。

2015年7月，参加全国信安标委组织的智慧城市信息安全标准相关项目讨论会。

2015年9月，全国信安标委组织对标准进行了专家评审，编制组吸收采纳专家意见继续修改完善标准。

期间向中国管理科学院、国家信息中心、国家保密科学技术研究所、公安部网络安全保卫局、浙江省商用密码管理局等多家单位征求意见。

2016年5月，全国信安标委在杭州召开第三届全国网络安全标准宣贯会，研究组在会上向来自全国各地20多个省市以及浙江省各地市、各部门及重要企业和相关单位介绍讨论标准草案并征求意见。

2016年6月，全国信安标委在北京举办全国信安标委第一次会议周，研究组在大数据标准组介绍标准项目情况并征求中国信息安全测评中心、国家信息安全工程技术研究中心、陕西省信息化工程研究院、陕西省网络与信息安全测评中心、IBM公司、南京中新赛克科技有限公司等多家单位的意见。

2016年8月，国家信息中心信息与网络安全部在四川省成都市组织召开“C3安全峰会政府行业及智慧城市网络安全论坛”。研究组在会上向来自全国各省市相关单位介绍标准草案并征求意见。

2016年9月，根据全国信息安全标准化技术委员会的要求参加在西安召开的《智慧城市网络安全评价方法》标准研究项目启动会，在会议上介绍《智慧城市建设信息安全保障指南》标准

研制情况并讨论征求意见；同时参与西安电子科技大学《智慧城市公共支撑与服务平台安全要求》标准研究、北京匡恩网络《智慧城市安全体系框架》标准研制、陕西省网络与信息安全测评中心《智慧城市网络安全评价方法》研究等项目讨论工作；对已立项智慧城市网络安全标准制定和研究项目中智慧城市相关的术语、技术参考架构等进行了协调统一。

2016年10月，全国信息安全标准化技术委员会大数据安全标准特别工作组2016年第二次会议周上，对《智慧城市建设信息安全保障指南》标准研制情况进行讨论征求意见。对标准内容中的智慧城市技术参考模型、安全框架，信息安全与其他安全域的关系框架图，网络安全、互联网安全以及关键信息基础设施保护之间的关系，本标准与信息安全等级的关系，标准部分附录等进行了质询和解答，编制组根据反馈意见修改标准文本。

2017年3月，组织专家对标准草案每条文本进行了审核讨论，根据专家评审意见，编制组修改标准文本，建议形成标准征求意见稿；完善标准研究编制说明。

2017年4月8日至11日，全国信息安全标准化技术委员会大数据安全标准特别工作组（SWG-BDS）2017年第一次会议在武汉市召开。会议讨论和审议通过智慧城市信息安全保障国家标准草案经修改完善后进入征求意见稿阶段；编制组根据会议意见修改完善标准文本，形成标准征求意见稿；完善标准研究编制说明。

## 2 标准研究编制的依据与指导思想

本规范研究编制的主要标准依据包括以下内容：



GB/T 25069-2010 信息安全技术 术语

GB/T 20269-2006 信息安全技术 信息系统安全管理要求。

GB/T 20945-2013 信息安全技术 信息系统安全审计产品技术要求  
要求和测试评价方法

GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20271-2006 信息安全技术 信息系统通用安全技术要  
求。

GB/T 20272-2006 信息安全技术 操作系统安全技术要求。

GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要  
求。

GB/T 20282-2006 信息安全技术 信息系统安全工程管理要  
求。

GB/T 21028-2007 信息安全技术 服务器安全技术要求。

GB/T 21052-2007 信息安全技术 信息系统物理安全技术要  
求。

GA/T 708-2007 信息安全技术 信息系统安全等级保护体系  
框架。

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本  
要求。

GB/T 28448-2012 信息安全技术 信息系统安全等级保护测评  
要求。

GB/T 22240-2008 信息系统安全等级保护定级指南。

GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计

技术要求。

GB/T 29245-2012 信息安全技术 政府部门信息安全管理基本要求。

### 3 主要技术内容介绍及分析

#### 3.1 总体思路

智慧城市是一项复杂的大型系统工程，其安全问题尤显重要：一方面，在未来网络时代未根本解决好安全问题的情况下，系统的信息感知层、接入与传送层、应用层与终端层、智能/智慧处理及协同平台层等诸多层面存在不安全因素；另一方面，不可或缺的云化支持与社会管理环境等也带来诸多突发性不安全因素。这些不安全因素可能会影响整个城市，导致工厂停产、商店停业、电气中断、交通瘫痪、水源切断等，使城市陷入一片混乱，造成极严重后果，因此必须倍加重视与小心务实应对。

为推进在我国智慧城市建设，指导基于物联感知、海量数据的智慧城市信息安全保障工作，特制定本指导性技术文件。本指导性技术文件确立了智慧城市信息安全保障架构，对智慧城市项目建设信息安全保障架构所涉及的各阶段的业务应用、数据、网络、物理等提出了相关要求。

本指导性技术文件适用于政府部门或项目单位智慧城市信息安全设计工作，为智慧城市管理人员、工程技术人员等相关人员进行信息安全建设提供管理和技术参考。

#### 3.2 适用范围

本指导性技术文件确立了智慧城市建设全过程的信息安全保障体系，包括智慧城市建设从规划与需求分析、勘察设计、实施施工、检测验收、运营维护、监督检查与评估到优化与持续改进的全过程信息安全保障的责任体制建设与技术规范指南。在全面落实已有信息化建设安全标准规范的基础上，针对云计算、物联网、移动互联网、大数据等智慧城市信息技术，制定信息安全保障管理规范与技术规范框架，明确智慧城市建设信息资源交换整合、提升应用所涉及的安全域、信息设备产品、信息系统、数据资源以及运维检测等方面的安全保障规范。

本指导性技术文件适用于智慧城市管理、建设、运营及运维单位，为智慧城市管理人员、工程技术人员等相关人员进行信息安全设计、建设及运维提供管理和技术参考。

### 3.3 主要内容

本指南主体内容由智慧城市信息安全概述，智慧城市安全保障机制，智慧城市建设全过程安全保障管理要求和智慧城市建设信息安全保障技术要求的 4 章正文，智慧城市风险评估方法和流程、信息分类分级管理、安全域划分与管理等 3 个规范性附录，信息安全建设内容编制要求、智慧城市建设项目信息安全评估要求、智慧城市建设项目信息安全审核要求、智慧城市终端安全要求、智慧城市一体化网络平台安全要求、安全管理平台技术要求、无线技术安全要求以及密码技术要求等 8 个资料性附录组成。

智慧城市概述包括：智慧城市整体架构及其主要特征的内容说明、智慧城市风险分析、智慧城市安全框架 4 节。

智慧城市安全保障机制包括：智慧城市安全体系建设主要角色与责任划分，建立责任人机制，追溯查证机制，监督检查机制，应急预案演练与处理机制，服务外包安全责任机制，信息安全保障教育培训机制等 7 节。

智慧城市建设全过程安全保障管理要求包括：政策制定与监督，信息安全保障规划，信息安全保障需求分析，信息系统安全保障设计，信息系统实施安全保障，信息系统安全检测验收，信息系统运行维护安全保障，信息安全保障优化与持续改进 8 节。

智慧城市建设信息安全保障技术要求包括：计算环境安全要求，通信网络安全要求，终端安全要求，应用安全要求，数据安全要求，密码技术要求，安全产品要求，智慧城市产品安全接口要求，一体化安全维护管理平台，物品标识认证要求等 10 节。