

《数字政府信息技术服务供应链安全要求》 (送审稿)编制说明

一、项目背景

近年来,全球软件供应链安全事件频发,影响面也越来越大,软件供应链安全已成为网络空间攻防对抗的焦点,数字城市软件供应链安全也面对前所未有的安全威胁和复杂情况,风险已遍布城市化所有场景之中,影响数字经济发展,甚至危害社会安全 and 国家安全。

国际方面,国际社会一直在高度关注软件供应链的安全性。2018年11月15日,美国国土安全部(DHS)宣布成立了信息和通信技术(ICT)供应链风险管理(SCRM)工作组;2019年5月15日,美国将关于保护信息和通信技术及服务供应链安全的第13873号行政命令(E0)签署成为法律;2021年美国总统一拜登发布关于增强国家网络安全的14028号政令,提高软件供应链的安全性和完整性;2023年9月25日,美国网络安全和基础设施安全局(CISA)发布了信息和通信技术(ICT)供应链风险管理工作组针对供应链风险管理产品的新硬件物料清单框架。

国内方面,国家高度重视软件供应链安全,习近平总书记曾经指出“供应链的‘命门’掌握在别人手里,那就好比在别人的墙基上砌房子,再大再漂亮也可能经不起风雨,甚至会不堪一击”。近年来相关软件供应链政策法规、标准规范陆续出台,2020年

多部门联合出台了《网络安全审查办法》该法规一经出台和执行，为软件产品测试、交付等供应链环节提供了法律保障；2022年11月7日，发布《信息安全技术 关键信息基础设施安全保护要求》对“软件供应链安全”提供明确要求；2024年4月，发布《网络安全技术 软件供应链安全要求》，提出软件供应链安全风险管理体系并持续改进，防范软件供应链中的供应关系风险要求。

我国多项相关标准规范发布，标志软件供应链安全保障体系已初步建立，但现有软件供应链相关标准尚未针对信息技术服务供应链各个环节的安全事件和安全风险形成针对性的防范措施和规范要求。数字政府信息技术服务存在供应链环节多、实施周期长、相关软硬件复杂、服务人员流动频繁等特点，伴随着云计算、区块链及大模型等前沿新型技术不断涌现，也给数字政府带来新的安全挑战，因此开展本文件的研制工作。

本文件在现有软件供应链相关标准的基础上进行细化和扩展，针对当前政府数字化建设过程的软件开发与集成、运营与维护、数据治理及信息技术咨询等信息技术服务采购工作，及其面临的服务规划风险、服务入场风险、服务实施风险和服务结束风险等，提出安全要求。本文件的制定和实施，有助于帮助数字政府明确信息技术服务供应链安全基线，全面提升全市党政机关及重要部门信息技术服务供应链安全风险防范与事件处置水平，为数字政府新质生产力高质量发展保驾护航。

二、工作简况

（一）任务来源

根据 2024 年 4 月 7 日《深圳市市场监督管理局关于下达 2024 年深圳市地方标准计划项目任务的通知》立项，文件立项名称为《数字政府信息技术服务供应链安全要求》。

（二）主要起草过程

1. 项目预研阶段

2023 年 9 月，深圳市信息安全管理中心作为牵头单位成立标准编制组，建立工作联络机制，开展筹划立项。标准编制组对国内外信息技术服务供应链安全相关标准政策现状、信息技术服务供应链安全现状及发展趋势、深圳市数字政府信息技术服务安全现状等内容进行调研分析，初步确定标准编制思路与框架内容。在此基础上邀请了多名重要行业专家进行技术研讨，与会专家针对标准编制思路、主体内容、具体技术细节等方面提出多项建议。

2023 年 10 月至 2024 年 1 月，标准编制组初步形成标准草案，并继续组织本领域及行业安全专家对标准草案进行研讨，后根据专家意见进一步修改完善了标准草案。

2. 项目立项阶段

2024 年 3 月，深圳市信息安全管理中心提交《深圳市地方标准制修订计划项目建议书》，2024 年 4 月 7 日深圳市市场监督管理局批准立项。

3. 编制起草阶段

2024 年 4 月至 2024 年 7 月，深圳市信息安全管理中心组织内部专家及其他参与起草单位对标准草案再次进行研讨和交流，根据评审意见，不断完善标准文本，形成标准征求意见稿。

三、地方标准主要内容的依据以及与国内领先、国际先进标准的对标情况

（一）标准编制原则

本文件在编制过程中遵循以下原则：

1. 合规性原则

本文件遵从软件供应链安全有关法律法规的规定，条款内容符合我国法律法规和相关政策要求。

2. 实用性原则

本文件在编制过程中，综合考虑深圳市数字政府信息技术服务供应链安全需要，在充分全面的调研基础上开展，使得内容更贴近实际需要，保证可操作性。

3. 先进性原则

本文件在编制过程中，充分调研国内外相关技术要求，保证内容的技术先进性。

（二）标准主要内容的依据

本文件的编制，主要引用如下规范性文件：

GB/T 2887—2011 计算机场地通用规范

GB/T 9361—2011 计算机场地安全要求

GB/T 22239—2019	信息安全技术	网络安全等级保护基 本要求
GB/T 28458—2020	信息安全技术	网络安全漏洞标识与 描述规范
GB/T 30276—2020	信息安全技术	网络安全漏洞管理规 范
GB/T 30279—2020	信息安全技术	网络安全漏洞分类分 级指南
GB/T 31168—2023	信息安全技术	云计算服务安全能力 要求
GB/T 32400—2015	信息技术	云计算 概览与词汇
GB/T 32914—2023	信息安全技术	网络安全服务能力要 求
GB/T 32926—2016	信息安全技术	政府部门信息技术服 务外包信息安全管理规范
GB/T 34943—2017	C/C++语言	源代码漏洞测试规范
GB/T 34944—2017	Java语言	源代码漏洞测试规范
GB/T 36637—2018	信息安全技术	ICT供应链安全风险管 理指南
GB/T 39412—2020	信息安全技术	代码安全审计规范
GB/T 39770—2021	信息技术服务	服务安全要求

GB/T 42446—2023 信息安全技术 网络安全从业人员能力基本要求

（三）与国内领先、国际先进标准的对标情况

1. 与国内领先标准对比

国家标准层面，GB/T 29245—2012《信息安全技术 政府部门信息安全管理基本要求》规定了政府部门信息安全管理基本要求，用于指导各级政府部门的信息安全管理工作；GB/T 32926—2016《信息安全技术 政府部门信息技术服务外包信息安全管理规范》建立了政府部门信息技术服务外包信息安全管理模型，提出了政府部门信息技术服务外包信息安全管理生命周期各阶段活动的管理要求；GB/T 36637—2018《信息安全技术 ICT供应链安全风险管理指南》规定了信息通信技术供应链的安全风险管理过程和控制措施；GB/T 43698—2024《网络安全技术 软件供应链安全要求》给出了软件供应链安全保护目标，规定了软件供应链组织管理和供应活动管理的安全要求。整体来看，多数仅对软件供应链或服务外包提出风险管理要求，未考虑数字政府领域系统集成、安全运维、数据加工处理、云计算服务、大模型算力等多种信息技术服务模式。

针对深圳数字政府建设现状，本文件在国家标准基础上，结合深圳市的实际情况进行进一步细化和扩展，为深圳数字政府信息技术服务供应链提供安全管理指导。

2. 与国际先进标准对比

国际标准化组织（ISO）和国际电工委员会（IEC）在信息技术外包安全管理方面进行了一系列研究。ISO 37500《外包指南》基于客户与供应商共同利益，阐述了外包模型、外包治理框架、外包战略（策略）分析、外包的启动与选择、外包准备工作的过渡（移交）、外包执行与价值交付等内容。ISO 27036—3《ICT供应链安全指南》表述了供应链安全的关键概念和实践，围绕协议过程、项目使能过程、项目过程、技术过程四个供应链生命周期的过程，阐述了25个具体过程及150个活动，适用于对供应链（外包）过程的安全管理。

美国国家标准与技术研究院（NIST）也制定了NIST SP800—161标准，指导美国联邦机构识别、评估、选择、实施ICT供应链风险管理过程。

以上国际标准对于供应链风险管理做出规范指导，但与我国数字政府发展背景差异较大，缺少针对性和适用性，本文件在借鉴ISO/IEC、NIST等相关国际标准的基础上提出更具有针对性的数字政府信息技术服务供应链安全要求。

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

（一）主要条款说明、技术指标参数

文件主要针对数字政府信息技术服务供应链供需双方实体角色分别提出通用安全要求和扩展安全要求，整体内容共分为6个章节，包含5个附录，以下对文件的主要条款进行简要说明。

1. 范围

文件规定了数字政府信息技术服务供应链的通用安全要求，以及开发与集成服务、运营与维护服务、基础设施服务、大模型服务与其他服务供应链的扩展安全要求。文件适用于指导数字政府范围内非涉密信息技术服务的供应链安全管理，也可为政府部门的数字政府信息技术服务供应链安全评估和监督检查提供规范性依据。

2. 规范性引用文件

对本文件规范引用进行说明。

3. 术语和定义

对本文件适用的术语进行了说明。

4. 数字政府信息技术服务供应链安全要求概述

本文件定义了数字政府信息技术服务类型，包括开发与集成服务、运营与维护服务、基础设施服务、大模型服务和其他服务等；本文件给出了数字政府信息技术服务供应链安全目标；本文件明确了信息技术服务供应链安全管理基本原则。

本文件提出了如下图所示的信息技术服务供应链安全要求的内容框架：

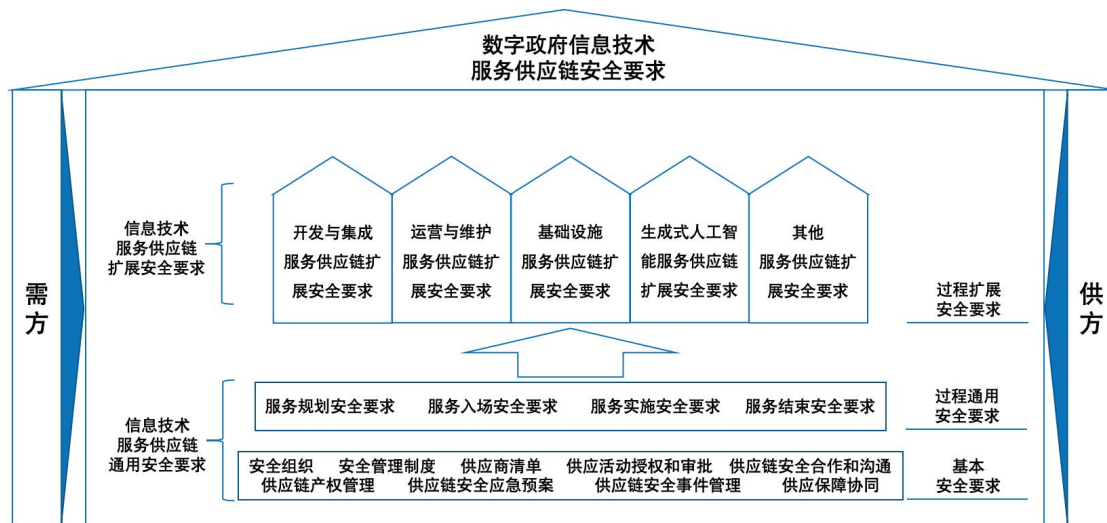


图 1 信息技术服务供应链安全要求框架

5. 需方信息技术服务供应链安全要求

给出了需方的数字政府信息技术服务供应链安全要求，包括通用安全要求和扩展安全要求。

通用安全要求包括基本安全要求和服务过程安全要求。其中基本安全要求包括组织机构、安全管理制度、供应商清单、供应活动授权和审批、供应链安全合作和沟通、供应链产权管理、供应链安全应急预案、供应链安全事件管理、供应链安全检查评估共九项内容，服务过程安全要求包括服务规划、服务入场、服务实施、服务结束阶段的安全要求。

扩展安全要求包括开发与集成服务、运营与维护服务、基础设施服务、大模型服务、其他服务共五类在服务规划、服务入场、服务实施、服务结束阶段的差异化安全要求。

6. 供方信息技术服务供应链安全要求

给出了供方的数字政府信息技术服务供应链安全要求，包括

通用安全要求和扩展安全要求。

通用安全要求包括基本安全要求和服务过程安全要求。其中基本安全要求包括组织机构、安全管理制度、次级供应商清单、供应链安全合作和沟通、供应链产权管理、供应链安全应急预案、供应链安全事件管理、供应保障协同八项内容。服务过程安全要求包括服务规划、服务入场、服务实施、服务结束阶段的安全要求。

扩展安全要求包括开发与集成服务、运营与维护服务、基础设施服务、大模型服务、其他服务共五类在服务规划、服务入场、服务实施、服务结束阶段的差异化安全要求。

7. 附录

给出了信息技术服务供应链安全要求与其他法律法规技术标准的对应关系、数字政府信息技术服务供应链通用要求对应安全风险、数字政府信息技术服务供应链扩展要求对应安全风险三项资料性附录及数字政府信息技术服务供应链安全评估计分、数字政府信息技术服务供应链增强安全要求两项规范性附录。

（二）主要试验情况分析

本文件在编制过程中，选取了深圳市典型单位、典型业务场景作为试点，通过评估验证方式开展试验。已在深圳市宝安区政务服务和数据管理局、深圳市福田区政务服务和数据管理局、深圳市龙岗区政务服务和数据管理局、深圳市财政局、深圳市市场监督管理局等 15 家单位开展了供应链安全评估工作，各试点单

位结合供应链安全评估报告，梳理各自风险情况，研究提交标准修改意见及标准推广思路等，推动完善标准文本。

五、是否涉及专利等知识产权问题

本文件不涉及专利及知识产权问题。

六、重大意见分歧的处理依据和结果

无。

七、实施地方标准的措施建议

本文件旨在为深圳市数字政府信息技术服务供应链供需双方提供安全管理指导，帮助信息技术服务供应链供需双方快速达成安全共识、建立安全意识，减少信息技术服务采购和实施过程中的安全隐患，提升信息技术服务供应链的安全性。可使用本文件对信息技术服务供应链的需方和供方进行安全管理和培训，同时本文件还可作为信息技术服务供应链安全管理的重要参考资料随时查阅。

对于本文件中能够进行自动化验证的安全内容，行业主管部门可配合合规性自证工具、供应商评估工具、配置安全检测工具、黑盒检测工具、容器镜像安全检测工具等，对信息技术服务供应链需方和供方的合规性进行检查，从而切实督促信息技术服务供应链供需双方提升安全性。

八、其他需要说明的事项

无。