ICS 35.030
CCS L 80

团　　体　　标　　准

T/CIIPA 00009—2024

关键信息基础设施供应链安全要求

Security capability requirements for the supply chain of critical information infrastructure

2025-03-07 发布　　2025-03-09 实施

中关村华安关键信息基础设施安全保护联盟　发布
中　国　标　准　出　版　社　出版

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村华安关键信息基础设施安全保护联盟提出。

本文件由中关村华安关键信息基础设施安全保护联盟网络安全标准专业委员会技术归口。

本文件起草单位：中关村华安关键信息基础设施安全保护联盟、中国工商银行股份有限公司、国网思极网安科技（北京）有限公司、中国电子科技集团公司第十五研究所信息产业信息安全测评中心、中国移动通信集团有限公司、中广核数字科技有限公司、中国人民财产保险股份有限公司、中国电力科学研究院有限公司、国家工业信息安全发展研究中心、中国电信集团有限公司、教育部教育管理信息中心、中国民生银行股份有限公司、北京北信源软件股份有限公司、中国信息安全测评中心、国家广播电视总局监管中心、工信部教育考试中心、中邮信息科技（北京）有限公司、大唐科技研究总院、水利部信息中心、深圳市网安计算机安全检测技术有限公司、四川北斗弘鹏科技有限公司、北京安普诺信息技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、银行卡检测中心（北京银联金卡科技有限公司）、杭州默安科技有限公司、杭州中尔网络科技有限公司、北京比瓴科技有限公司、深圳开源互联网安全技术有限公司、湖南浩基信息技术有限公司、南京众智维信息科技有限公司、成都久信信息技术股份有限公司。

本文件主要起草人：苏建明、郭启全、焦彬、逯瑶、马强、李红霞、郭智武、林皓、杨华、张松、徐建、任磊、严宗、肖红阳、马雅静、曹禹、刘阳、刘冬、胡建勋、伊鹏达、刘云、张然、吴子坚、陈军、陈大北、马禹昇、郑国忠、王雪珊、李淼、白云波、张普含、李天磊、詹丹丹、裴帅、刘健、冯莉、李炎、谭志彬、苏勇、张仕文、曹欣然、盛湘新、沈智镔、陈真玄、邱德隆、王来蒙、王文军、张涛、宁戈、李云、任航、付杰、聂万泉、孟瑾、沈锡镛、邹远辉、曾帅、刘遥、谭宇辰、冯寅轩、营志刚、车洵。

引　言

目前，关键信息基础设施已成为国家安全、经济稳定运行和社会公共服务的重要基石，其供应链安全性问题日益凸显，直接关系到核心数据和整个系统安全。近年来，供应链已成为黑客攻击的关键环节，任何供应链环节的疏漏都可能对整体安全构成严重威胁。网络攻击者常利用对目标漏洞的深入了解，辅以先进的技术和工具，对供应链发起攻击，特别是对开源软件漏洞的利用，已成为攻击者渗透网络系统的重要途径。随着开源软件的广泛应用，软件供应链攻击的成本和难度大幅降低，而攻击范围却在不断扩大，检测难度日益增加，攻击事件的数量也呈持续上升趋势。

鉴于此，关键信息基础设施供应链安全的重要性不言而喻，它不仅关乎个体的数据安全，更涉及国家安全、经济安全和社会公共服务的稳定运行。为了全面提升关键信息基础设施供应链安全能力，有效防范和控制供应链引发的重大网络安全威胁，亟需制定一套科学、系统、实用的供应链安全能力规范。

本文件的制定旨在规范关键信息基础设施的供应链安全管理，为关键信息基础设施运营者及网络安全服务机构等提供明确的指导和要求。通过健全完善供应链安全管理制度，落实供应链安全管控措施，加强防范供应链风险能力，构建一个更加安全、可靠、高效的关键信息基础设施供应链体系，为国家网络安全保驾护航。

关键信息基础设施供应链安全要求

1 范围

本文件规定了关键信息基础设施的供应链安全总体要求、风险识别、管控要求、准入要求和外部组件的供应链安全管理要求。

本文件适用于指导CII运营者对关键信息基础设施开展供应链安全防护，也为网络安全服务机构制定供应链安全解决方案提供参考。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

关键信息基础设施 critical information infrastructure；CII

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

[来源：GB/T 39204—2022，3.1]

3.2

供应链 supply chain

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立连续供应关系的组织系列。

注：其中每一组织充当需求方、供应方或双重角色。

[来源：GB/T 39204—2022，3.2]

3.3

需求方 acquirer

从其他组织获取产品和服务的组织。

注1：获取可能涉及或不涉及资金交换。

注2：重要信息系统和关键信息基础设施的运营者，通常是从供应方获取产品和服务的需求方。

[来源：GB/T 36637—2018，3.1，有修改]

3.4

供应方 supplier

提供产品和服务的组织。

注1：供应方也可称供应商。

注2：供应方可以是内部的或外部的组织。

注3：供应方包括产品供应商、服务提供商、系统集成商、生产商、销售商、代理商等。

[来源：GB/T 36637—2018，3.2，有修改]

3.5

供应链安全风险　supply chain security risk

供应链安全威胁利用供应链管理中存在的脆弱性导致供应链安全事件的可能性，及其由此对组织造成的影响。

[来源：GB/T 36637—2018，3.5]

3.6

构件　component

构成产品或信息系统的部分，可以是硬件或软件且可以进一步划分为其他部件。

注 1：构件也可称部件。

注 2：可以是成熟的、可重用的部件。

注 3：术语“模块(module)”、“部件(component)”、“单元(unit)”常常可以互换使用或在不同的方法中，定义作为另一个的子元素，取决于上下文。这些术语的关系尚未标准化。

注 4：在软件工程中，构件包含使用的外部组件。

[来源：GB/T 11457—2006，2.261，有修改]

3.7

外部组件　external component

由供应方以外的组织或人员开发的程序代码、文档或数据，通常由二进制程序文件或者源代码程序文件构成。

注：外部组件包括软件中使用的开源组件和第三方组件。

[来源：GB/T 43698—2024，3.11]

4　CII 供应链安全总体要求

4.1　供应链安全风险分析

实施供应链安全管理，识别供应方、使用人员、以及提供的产品、服务中存在的安全风险，从需求方视角对供应方的选择与经营能力、人员的选用与退出等多方面风险进行了识别，并重点对产品的研发、供应和运维环节，以及服务装备和方式等多个层面进行了详细分析，为安全管控的要求提供依据。

4.2　供应链安全管控措施

从四个方面开展供应链的安全管控，应对安全风险。一是对实施审查过程管理的要求，确保供应链安全管理各环节都受到严格的审查和监管；二是对安全管理建设层面提出要求，确保管理工作的高效、有序开展，为各环节提供必要的支持和保障；三是对使用技术管控手段提出安全要求，及时发现并处置潜在安全问题；四是从人员的安全管理层面提出要求，降低人员使用风险，确保具备必要的安全意识和技能。

4.3　供应链安全准入策略

安全准入作为供应链安全管理全生命周期中最重要的一环，从供应方、人员、产品和服务四个方面制定了具体的规范要求，保障在供应方筛选、人员的选择和管理、以及产品和服务的准入方面具备可执行性，明确安全责任。

4.4　外部组件供应链安全要求

在供应链安全管理中，外部组件的使用由于没有明确的供需求方合同约束，需求方应加强自身的管理约束，从组件获取、使用、更新、风险监测等方面提出了相应的安全管控要求，包括源代码安全、第三方