ICS 00.000
X XX

CIIPA

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

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中关村华安关键信息基础设施安全保护联盟　发布

目　　次

前　言

本文件按照《中关村华安关键信息基础设施安全保护联盟标准管理办法（暂行）》的要求，依据 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和解释。

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、杭州漠坦尼科技有限公司、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、焦彬、逯瑶、马强、李红霞、郭智武、林皓、杨华、徐建、任磊、严宗、肖红阳、马雅静、曹禹、刘阳、刘冬、刘元、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、孙茂增、王天昊、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、谢金鑫、彭洋、胡健勋、谭宇辰、冯寅轩、菅志刚、车洵。

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中关村华安关键信息基础设施安全保护联盟（地址：北京市海淀区板井路 69 号世纪金源商务中心 607，100097，网址：http://www.ciipa.com，邮箱：guanbaolianmeng@cnciipa.com）。

引　言

随着信息技术的飞速发展，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，更涉及到国家安全、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。

本团体标准《关键信息基础设施供应链安全能力要求》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，我们期望构建一个更加安全、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能力要求

1 范围

本文件适用行业范围与 GB/T 39204《信息安全技术 关键信息基础设施安全保护要求》中对关键信息基础设施行业所定义的范围保持一致，细化了要求中“供应链安全保护”章节内容，形成可供各行业 CII 运营者参考使用的通用要求。

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，也可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

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 25069-2022 信息安全技术 术语

GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南

GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求

GB/T 42109-2022 供应链资产管理体系实施指南

GB/T 43698-2024 网络安全技术 软件供应链安全要求

3 术语和定义

3.1 关键信息基础设施 critical information infrastructure

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 信息安全技术 关键信息基础设施安全保护要求]

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 信息安全技术 关键信息基础设施安全保护要求]

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 信息安全技术 ICT 供应链安全风险管理指南，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 信息安全技术 ICT 供应链安全风险管理指南，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 信息安全技术 ICT 供应链安全风险管理指南]

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 信息技术 软件工程术语，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 网络安全技术 软件供应链安全要求]

4 缩略语

下列缩略语适用于本文件。

CII：关键信息基础设施（Critical Information Infrastructure）

5 CII 供应链安全总体要求

5.1 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。

5.2 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。

5.3 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，保障在供应商筛选、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。

5.4 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、第三方组件安全、集成与分发安全、可追溯性等四部分内容，对外部组件的使用与管理进行约束，明确了清单的使用要求，提升发现和处置问题隐患的能力。

6 CII 供应链安全风险识别

6.1 供应方风险

需求方在与供应方合作过程中，需求方应关注供应方的以下风险：

a） 供应方的机构属性及背景、政治倾向、机构组成成份、法人及核心管理层的国籍、任职情况等，避免政治风险；

b） 供应方的行业资质、经营范围及国内、国际制裁限制等，避免产生合规风险；

c） 供应方的生产、经营状况、知识产权状态、信誉、法律纠纷状况，避免出现无法履约的风险；

d） 与供应方的联络与数据交换方式、数据种类及知悉范围，避免出现数据泄露风险；

e） 供应方产品及服务的质量评价，避免出现影响需求方自身利益、声誉及品牌形象的风险；

f） 供应方的安全防护措施，避免出现由供应方引起的供应链安全风险；

g） 供应方在所属行业的发展趋势，避免出现供应商选择单一化、议价能力显著下降的风险。

6.2 人员风险

在需求方自主招募，或供应方提供人员技能服务的过程中，需求方应关注人员以下风险：

a） 人员的政治倾向、认证资质与背景状态（包括自身及亲属政治身份、学历、从业经历、项目经历、无犯罪记录、诚信记录等），避免人员出现安全及合规风险；

b） 人员的身份核验、权限、活动范围、行为操作等，避免出现安全风险；

c） 人员的工作的稳定性、技能水平和服务质量，避免出现生产效率及服务质量下降、无法按标准完成生产任务等风险；

d） 人员在服务过程中的工作方式、自身健康及情绪状态，避免出现隐私侵犯、数据泄露、协作或服务中断的风险；

e） 外部人员在支撑关键岗位过程中的数量占比，避免出现人员依赖及自主能力下降的风险；

f） 人员在退出服务后的安全教育与保密检查，避免出现安全事件或数据泄露的风险。

6.3 产品风险

6.3.1 产品研发环节

在与供应方合作开展产品研发过程中，需求方应关注以下风险：

a） 数据泄露及网络安全风险：

1. 开发环境安全防护不足，使用第三方托管仓库，或开发网络直接暴露在互联网环境下；
2. 重要或敏感产品的网络开发环境未作安全隔离，未做有效的网络接入管控；
3. 产品研发场所权限管控缺失，未对研发无关人员进行管控；
4. 私自与外部人员探讨产品开发进展及技术方案；
5. 未对研发文档实施有效管控，未对信息公开、交换、共享、销毁等重点环节等进行管理，缺乏保密管理手段。

b） 产品安全及技术风险：

1. 未遵守安全操作规范、安全开发流程、技术规范、变更管理等相关流程；
2. 软件类产品未对使用的研发工具、外部组件进行安全评估，或使用来源不明的组件；
3. 未对产品进行充分的兼容性评估和产品测试，未对关键模块或软件代码进行审查、安全评估；
4. 未对参与开发的人员进行技术能力评估和筛选，重要产品研发未开展统一的技术培训。

c） 产品质量及管理风险：

1. 供、需双方未建立完善的沟通机制、管理模式和制度、评估及检测机制等；
2. 供应方未提供稳定的资源投入和人员保障；
3. 未实施有效的研发材料管控；
4. 供应方缺乏完善的研发质量管理流程和质量管理体系标准。

6.3.2 产品生产供应环节

在产品引入后的持续供应过程中，需求方应关注以下风险：

a） 生产风险

1. 供应方不具备独立自主的产品生产能力，或核心构件生产能力，缺乏有效的供应链管理；

2. 不具备完善的生产、操作流程，对生产人员管理不到位，未对生产物料实施有效管理与监测；

3. 未对生产环境区域实施准入控制与安全监控，生产环境所在地安全保卫能力不足；

4. 生产环境所在地发生安全事故、社会性事件、或自然灾害等问题导致生产中断。

b） 供应延迟或中断风险：

1. 因供应方政治倾向变化，国内、外制裁行为等导致供应中断。

2. 供应方生产能力下降，导致供应能力不足出现中断；

3. 因不安全仓储行为，或使用不可靠、不安全的仓储商，导致供应延迟，或出现中断；

4. 供应或运输渠道发生人为事件或自然灾害导致渠道受阻。

c） 产品安全风险：

1. 未交付完整的物料清单，或交付的产品、安装包与交付测试的不一致、不完整带来的安全风险；

2. 交付时未能识别被篡改或者伪造的组件，该类组件可能带来后门、漏洞等安全隐患；

3. 交付渠道安全管理和防护不足，致使产品安装包或技术文档被篡改、泄露等；

4. 未按要求对产品或其部署环境进行安全和参数配置，或私自预装程序。

d） 产品质量风险：

1. 需求方未建立完善的产品监测和检测流程、或未按要求对产品进行质量监测和检测；

2. 供应方或合作方未对产品外部构件来源实施管控和检测；

3. 安全、检测技术落后，未能识别被替换、伪造的组件；

4. 未对产品开展充分的兼容性测试，在多产品集成或使用的过程中无法正常开展业务活动。

6.3.3 产品运维环节

在产品运行维护过程中，需求方应关注以下风险：

a） 运维延迟或中断风险：

1. 供应方因经营状况、人员变更、合规性问题等原因未能按时开展运维工作；

2. 因政治立场、国内外制裁、自然灾害等因素未能按时开展运维工作；

3. 因缺乏必要的沟通和协调机制未能及时开展运维工作；

4. 因缺乏人员、资金、相关设备或工具等因素导致运维延迟或中断；

5. 供应方缺乏应急响应预案或不具备及时响应能力，无法应对突发状况。

b） 运维过程中的安全风险：

1. 供应方未能及时处置产品存在的安全漏洞，或未能及时对系统依赖的中间件、数据库、操作系统、云服务、外部组件等进行安全检测和更新；

2. 需求方未能对运维过程中服务人员的行为进行有效监控，致使出现被植入后门、私装软件、非授权变更配置参数等安全问题；

3. 产品返厂维护过程中缺乏安全管理，致使出现被植入后门、替换、盗取数据等安全问题；

4. 运维人员未能按要求遵守安全保密和安全操作规范；

5. 需求方人员缺乏安全保密意识，泄露敏感信息（如系统口令、运维文档等）；

6. 供应方网络安全防护能力不足，无法有效防护网络攻击等外部威胁；

7. 供应方产品组件受到外部供应链攻击。

6.4 服务风险

6.4.1 服务装备

需求方应关注服务工具、设备或信息系统等服务装备带来的以下风险：

a） 装备的来源及获取方式，避免因政治、合规、安全等因素造成服务延迟或服务中断的风险；

b） 装备的操作流程和使用规范，如网络安全软件、检测设备等，避免不当操作所带来的使用风险；

c） 装备的安全漏洞或安全配置缺陷，避免攻击者利用漏洞和缺陷发起供应链攻击；

d） 具有互联网接入和数据存储能力的装备，避免存在恶意代码造成数据泄露的风险；

e） 供应方信息系统的网络安全防护措施，避免增加需求方网络暴露面。

6.4.2 服务过程

在服务过程中需求方应关注以下风险：

a） 应关注供应方接入需求方信息系统后的行为或操作，避免出现篡改或盗取生产数据、私自收集需求方数据等风险；

b） 应关注对需求方数据及文档类信息的访问，对生产数据库的操作，以及供应方对数据及文档类信息的存储或传输操作，服务结束后的清理工作，避免造成数据泄漏风险；

c） 远程服务过程中，应关注服务人员变更时的身份核验，避免造成网络安全风险；

d） 出入关键区域时，应关注视频监控的运行情况，以及人员的陪同过程，避免服务人员引起设备破坏、信息泄漏等风险；

e） 应关注所处环境的物理安全防护措施，避免因环境因素造成设备损失或人员伤害，影响服务质量或造成服务中断；

f） 应关注需求方人员的安全保密意识，避免无意识泄露敏感信息；

g） 多供应方同时开展服务时，应关注人员的管理、授权、信息隔离等问题，避免出现信息泄露、人身安全等多种风险。

6.4.3 服务方式

在供应方提供远程和现场的服务过程中，需求方应关注以下风险：

a） 现场参与人员的数量，以及现场的安全措施，避免出现人身安全问题导致服务中断风险；

b） 服务人员活动范围及网络接入点的管控，避免出现活动区域超限或网络安全风险；

c） 供应方在非现场服务中是否使用了受控的服务场所、远程访问路径、对远程访问工具的安全保护，避免因不安全的场所、路径或远程访问工具而遭受网络攻击；

d） 供应方在非现场服务中远程访问账户的身份验证和授权管理，防止未经授权访问带来的风险；

e） 现场及非现场服务共存时，数据的传递与网络隔离问题，避免造成数据泄露风险；

f） 服务人员的更替与轮换频次，避免无关人员接触项目所带来的安全风险。

7 CII 供应链安全管控要求

7.1 审查管理要求

本项要求包括：

a） 需求方应按照国家法律法规和关键信息基础设施保护工作部门、网络安全审查工作部门下发的有关要求建立网络安全审查体系，明确审查流程、责任部门及人员配置，该体系应涵盖从需求分析、产品选型、风险评估到审查决策的全过程；

b） 需求方应按要求对关键信息基础设施及其关联设施的采购开展网络安全审查预判工作，并遵循应审尽审原则，对影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查；

c） 审查不应存在“白名单”机制，重复采购同一种产品和服务仍然需要按照“一事一议”的原则开展网络安全审查预判和申报工作；

d） 需求方或者网络产品和服务提供者应当严格保护知识产权，并对在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及其他未公开信息承担保密义务，未经信息提供应方同意，不得向无关方披露或者用于审查以外的目的；

e） 网络安全审查期间，需求方和网络产品和服务提供者应严格遵循、认真执行网络安全审查要求，主动配合，如实、及时提交审查材料，并按照网络安全审查要求采取预防和消减风险的措施；

f） 需求方或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

7.2 安全管理要求

本项要求包括：

a） 需求方应针对供应方的政治风险制定跟踪及调研机制，并定期评估；

b） 需求方应制定供应链管理的总体方针和安全策略，说明供应链管理的总体目标、范围、原则和安全框架等；

c） 需求方应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，覆盖供应链生命周期中主要活动，指定或授权专职的部门或人员负责安全管理制度的建设、发布，实施版本控制，定期对制度的合理性和适用性进行评估并更新；

d） 需求方应设立专职的供应链安全管理部门或岗位，制定和执行供应链安全策略，协调各部门之间的工作；

e） 需求方应建立完善的供应链清单管理机制，建立包括供应商清单、产品物料清单、技术服务外购清单、产品外部构件清单在内的多种管控清单，并定期对清单进行更新和维护；

f） 需求方应提高技术供应来源的多样性，降低关键信息基础设施对单一供应商的依赖，并逐步提升本机构技术及工具的自主可控性；

g） 需求方应制定外部人员行为及服务过程监控制度，根据人员来源、服务类型、服务方式、以及服务对象等开展安全管控；

h） 需求方应建立数据安全管理体系，并对本机构在互联网的信息进行技术监控，禁止供应方使用并存储需求方数据，确需使用、留存的应经过需求方评估与审批；

i） 需求方应建立产品研发安全管控体系，覆盖产品研发全生命周期，规范研发人员行为，禁止私自公开产品研发信息（如技术方案、文档、源代码、研发进展、参与方信息等）；

j） 需求方应制定供应链安全审计与评估制度，对合作供应商及供应链中关键环节（如准入环节）进行技术审计，开展安全风险评估和分析，及时处置潜在风险，完善管理制度建设；

k） 需求方应建立供应链安全事件应急响应机制，识别供应链应急场景，制定应急响应预案，明确事件的报告、处理流程，以及恢复策略，并定期组织应急演练活动；

l） 需求方应建立外部协作机制与管理制度，促进供应链上、下游机构、行业组织及政府机构的信息共享与协同处置；

m） 需求方应建立产品或服务的准入、退出机制与管理制度，明确准入、退出流程与管理要求；

n） 需求方应为保障供应链安全配备足够的专业人员，定期进行培训与考核，并为安全管理提供充足的资金支持。

7.3 技术管控要求

本项要求包括：

a） 需求方应严格依照国家法律法规及安全标准开展关键信息基础设施建设，并定期开展系统脆弱性评估及测评，降低安全风险；

b） 需求方应加强对部署在租用机房的信息系统的物理安全、网络隔离及数据安全管控，禁止非本机构人员开展运维工作；

c） 针对新技术应用，需求方应加强技术的兼容性、安全及稳定性测试与评估，限制初次应用范围，制定完善的推广应用策略与回退策略；

d） 需求方应对软件类产品的研发工具实施安全评估，从正式授权渠道获取相关工具，对开源渠道获取的安全测试类工具应在安全环境下通过检验后再投入使用；

e） 需求方应自行或由第三方检测机构对软件类产品在投入使用前开展安全检测，检测内容应覆盖产品使用的外部构件及第三方协议；

f） 需求方应明确供应方的职责定位，采取最小权责和授权机制制定供应方人员访问控制策略，对访问策略进行定期维护；

g） 需求方应严格限制并管理外部设备的网络访问路径、访问时长、以及设备种类，禁止使用非本机构设备对信息系统开展技术服务，确需使用的应采取必要的技术手段监控、审核、记录外部人员的网络访问及服务操作；

h） 需求方应使用技术措施管理供应方的产品或服务，建立产品、服务标识（如编码、条码、ID或者组织自定义的其他标识）；

i） 需求方宜对供应方建立账户管理体系，实施用户管理、角色管理、权限和授权管理及身份鉴别等措施，当供应方发生变更时，及时更新访问控制权限；

j） 需求方宜使用技术手段管理供应链资产清单，建立可追溯基线，并使用密码技术对清单信息的完整性和真实性进行保护；

k） 需求方宜建立供应链安全监控系统，覆盖供应商、供应渠道及第三方渠道等，及时响应和处理安全事件。

7.4 人员管理要求

在需求方对自身与供应方的人员和团队、外包及第三方人员实施管理时，应遵循以下基本要求：

a） 需求方应依照本机构的安全管理规定对人员的引入、使用和退出进行管理，明确各自的职责、权限和分工，必要时应签订保密协议；

b） 需求方应对人员的资质和能力进行审核，定期开展能力评估，并对关键岗位人员实施背景调查；

c） 需求方应按照最小必要和职责分离原则，严格管理供应链相关人员的权限，并实施定期审查，人员变动时应当及时调整权限或者收回账号；

d） 需求方应针对人员和团队特点制定不同的培训计划，对安全基础知识、安全意识教育、岗位技能和岗位操作规程进行培训，并告知相关的安全责任和惩戒措施；

e） 需求方应对人员的关键操作行为进行监控，保留审计日志。

8 CII 供应链安全准入要求

8.1 供应方准入要求

本项要求包括：

a） 对供应方机构的选择应符合国家的管理要求（如相关资质管理要求、销售许可要求等）；

b） 需求方应制定本机构的供应方筛选策略和制度，对供应商进行准入评估，包括但不限于政治倾向、机构背景、股权关系、基本信息、财务状况、技术能力、人员、资质审查等内容，建立符合本机构的供应方准入基线；

c） 需求方应建立多元化的供应方目录，并及时更新和维护：

1. 目录的维护应充分考虑多方面因素，包括政治、外交、贸易、经济、供应方自身经营状态因素，以及各国家、地区的法律、法规变化、文化等；

2. 需求方应建立供应方信用评价标准，根据合作表现对供应方进行评价，为目录维护及后续合作提供参考依据；

3. 需求方应定期对目录中已开展合作的供应方进行审查，并建立目录的维护与审核保障机制，根据本机构的供应方风险评估及考核结果，及时更新目录；

4. 需求方宜定期开展供应方调研，对其管理、技术、研发能力，发展方向、经验积累等进行评估，并更新供应方目录信息。

d） 需求方应制定供应方风险管理机制，以及对供应方的监督、考核与违规处理制度，定期开展考核与监督工作，筛选安全可靠的供应商；

e） 需求方在公开征集、选择供应方时，应在满足国家有关管理要求的基础上，对本机构额外要求进行明确，并通过签订合同或协议的方式进行约束，额外要求不限于以下内容：

1. 产品或服务的质量保障、交付周期及时限要求、产品或服务变更要求等；

2. 需要额外签订的责任、权限、义务、服务承诺、以及相互通报内容与约束等；

3. 需提供的技术资料，培训支持、服务人员组成及应急响应支持等；

4. 对供应方产品供应链的额外要求与承诺，以及供应方应具备的管理、研发机制与管控措施等；

5. 供应方的安全保障要求或承诺，内容不限于履行网络安全和保密责任，不得设置后门、非法操作或谋取不正当利益等。

f） 针对关键或特殊场景使用的产品或服务，应考虑以下因素：

1. 满足国家法律、法规及监管的安全要求，对可能影响国家安全的应依照规定开展审查；

2. 国家已发布的限制及准入条件，供应商清单，或指定的相应机构；

3. 供应方的安全管控措施，其供应链渠道及组织运转过程的透明度，使用可信或可控的分发、交付和仓储手段；

4. 关键产品构件或服务来源的安全性、可控性，交付及交付周期的稳定性。

8.2 人员准入要求

本项要求包括：

a） 需求方应根据自身需求设置不同岗位人员筛选条件（如人员背景、政治倾向、学历、从业履历、职业资格证书等），并对其相关证书进行验真；

b） 需求方应根据自身情况建立人员考核机制，使人员符合岗位准入要求；

c） 对于可接触到需求方重要系统、数据及岗位（含关键岗位）的人员，需求方应对人员进行背景审查，对于特殊行业、岗位还应进行保密审查，审查未通过的人员不得从事相关岗位工作；

d） 需求方应明确人员的保密要求，在完成签订保密协议后方可参与相关工作；

e） 使用外部人员应符合国家、行业及监管部门的安全管理要求，对人员数量占比进行管控，并对外部人员更换条件、频率等进行约束。

8.3 产品准入要求

本项要求包括：

a） 需求方应设置产品筛选条件（如性能、型号、样式等），对于需要产品认证资质的，应检查产品所具备的认证结果的真实性（如国家强制性认证、网络安全产品认证、商密产品认证、行业认证、ISO 系列认证等），影响国家安全的产品应通过国家网络安全审查；

b） 需求方应对产品功能进行测试与安全评估，制定合格基准线，或由供应方提供可信第三方机构出具的安全检测报告；

c） 供应方产品应具备详细的产品说明书，配置与用户文档，可提供外部构件清单以及任何有助于用户安全使用产品的操作方法、安全事项或说明材料；

d） 需求方应对影响产品安全或使用的主要外部构件实施准入管控，建立管理清单：

1. 应选择可信赖的外部构件来源，并开展安全评估，涉及核心构件的应及时建立替代方案；
2. 应用于关键场景或系统的产品，其外部构件中涉及开源软件或第三方组件的，应对此部分进行安全检测与评估，或由供应方提供可信第三方机构出具的安全检测报告；
3. 应对外部构件的知识产权状态、使用及安全状态进行评估，及时通报存在的风险；
4. 针对必须使用且暂时无法替代的外部构件，应评估其影响，对可能影响国家安全的应上报有关监管机构，开展安全审查。

e） 需求方应对涉及产品自身安全能力的功能、参数、或更新方案实施检查，要求供应方实施默认安全配置，提供及时有效的后续维护和应急响应方案；

f） 针对延续性产品准入，需求方应综合评估现产品质量与售后反馈，作为后续引入的参考或依据；

g） 针对供应方或产品突发变更或供应中断，需应急实施替换的产品，需求方应对新产品的使用进行安全风险评估，采取有关措施降低风险，实施风险管控后方可准入；

h） 需求方应对产品集中度风险进行评估和控制，审慎引入集中度风险较高或增加需求方整体网络安全风险的产品。

8.4 服务准入要求

本项要求包括：

a） 需求方应设置服务筛选条件（如服务标的、服务时长、模式等），明确关键服务要求、服务质量评价标准、知识产权归属、保密条款、违约责任等重要事项，并以协议的形式进行约束；

b） 对于需要服务认证资质的，需求方应检查供应商所具备认证结果（如国家强制性认证、行业认证，权威机构颁发的服务资质证书、人员资质证书等）的真实性；

c） 需求方应对服务提供商的人员数量、人员稳定性和专业能力进行约束，必要服务岗位或服务内容需签订保密协议；

d） 需求方应对服务范围、以及人员必要活动范围与权限进行限定，不得服务于核心职能岗位；

e） 针对延续性服务的准入，应综合评价现有服务供应方的服务成果，作为后续引入的参考或依据；

f） 针对供应方或服务突发变更或中断，需实施服务应急时，需求方应对新服务供应方或服务人员进行安全风险评估，采取有关措施降低风险，实施风险管控后方可准入。需求方应对供应方的信息安全管理能力进行评估，保障服务过程中涉及的敏感信息得到妥善保护；

g） 需求方应严格控制临时性服务的使用频次。

9 CII 外部组件供应链安全管理

9.1 开源组件安全管理

本项要求包括：

a） 需求方应建立开源组件引入和审核体系，完善管理、操作流程，明确管理责任和权限；定期开展审查，审查内容包括但不限于：代码的安全性、合规性、稳定性等方面，审查可由内部团队或第三方专业机构开展，出具审查结论及改进意见，及时调整安全管控策略和措施；

b） 应使用受控的代码管理工具并实施安全检测，禁止代码管理工具连接互联网，或使用第三方托管平台，对开源组件源代码实施版本化管理，使用最新、或者稳定版本，记录源代码的版本变更历史，及时更新补丁；

c） 应根据已公开信息或使用技术措施，对引入的源代码进行测试与安全检测（如白盒测试、漏洞扫描、恶意代码检测等），修复已公开漏洞，删除恶意代码；

d） 应对开源代码实施访问控制，限制人员的操作权限（如访问、更新、修改、删除等），记录操作行为，及时排查异常行为；

e） 在二次开发过程中，应遵循安全开发原则和规范，覆盖开发过程的全生命周期；

f） 应建立代码泄露监测和安全应急响应机制，及时处置源代码存在的安全问题，降低安全事件的影响；

g） 针对合作开发过程中引用的开源组件，应明确需求方与供应方的安全责任和管理权限，并以协议形式加以确认；

h） 应对使用的开源组件进行起源性追溯，对于可追溯至源头的应建立完整的传递关系，确认组件的作者身份，对于无法追溯至源头的应停用，并另寻或研发可替代组件；

i） 应采取措施对源代码的配置进行规范与管理，保障配置的安全性和一致性；

j） 应对软件工程研发团队进行定期的安全技能和意识培训。

9.2 第三方组件安全管理

本项要求包括：

a） 应选择可信赖的第三方组件来源，禁止使用未知或未经验证的组件，优先使用稳定版本；

b） 应建立跟踪与通报机制，对第三方组件的知识产权状态、使用及安全状态进行跟踪，及时通报存在的风险，组织并实施更新、修复、替换组件等处置措施；

c） 针对非自主可控的第三方组件，应丰富来源的多样性，降低此类组件的占比，对长期缺乏维护或即将废止的组件建立风险处置预案和实施计划，核心组件应及时建立替代方案；

d） 应对第三方组件进行功能及安全检测、评估和合规性检查，并在使用过程中定期进行检测，及时发现并处理存在的安全问题；

e） 针对重要应用场景或系统，供应方应提供详细的第三方组件安全证明材料（如安全测试报告、漏洞修复记录等）；

f） 宜建立本机构内部第三方组件库，存放通过安全性测试与评估的组件，制定使用说明文档，并及时更新库内组件。

9.3 集成和分发的安全管理

本项要求包括：

a） 应制定详细的安全集成方案，明确集成步骤、方法、测试与验证目标，对集成后的系统及时开展安全评估，并对系统性能、稳定性、以及安全性进行测试；

b） 应对集成与分发操作进行审批控制，实施权限管控；

c） 应采取安全的分发方式（如使用加密传输、数字签名与证书等），保障分发过程中组件的真实性、完整性和保密性，并遵守当地监管部门、知识产权、以及相关法律、法规的要求，管控分发范围；

d） 应定期对集成和分发的管控措施与流程进行评估与更新，并建立跟踪和反馈机制，及时了解组件在分发后的使用情况，发现并处置异常情况；

e） 应对接收分发产品的用户进行明确的安全告知，包括使用方法、安全注意事项等。

9.4 可追溯性管理

本项要求包括：

a） 应建立可追溯性的策略和管控流程，以及外部组件资产清单，记录外部组件的引入信息和组件属性（如原始供应方、开源社区、版本，开发贡献者、数字证书源、依赖关系等），并保留变更数据（如变更时间、内容、原因等），所记录信息可追溯至上游供应方，核心组件应追溯至源头供应方；

b） 应采用技术措施对组件的变更、集成和分发等操作日志进行保留与保护，防止信息被篡改；

c） 应定期对产品的外部组件依赖关系进行维护，识别直接与间接依赖，保障依赖关系的准确性，及时处置依赖冲突、许可证兼容冲突等问题；

d） 应采用管理或技术措施及时保障资产信息的准确性与供需双方间沟通的及时性；

e） 应记录涉及外部组件的安全事件处置信息（如事件时间、处置过程、结果、人员、影响范围等），并采用技术措施保护相关信息的完整性。