# 北京市开源软件供应链发展建议

伴随着产业发展，现代软件已经从单体模式演进到以开源软件为代表的规模化协作模式。复杂软件往往涉及诸多开源软件，这些开源软件彼此组合、依赖，连同为各个开源软件做贡献的维护者和开发者，共同形成一个包含上万个节点的供应关系网络，即开源软件供应链。建设和维护自主、安全、可靠的开源软件供应链是当今我国科技发展的重要保障。目前国内包括 openEuler、OpenAnolis、OpenHarmony 在内的诸多开源社区蓬勃发展，也有许多新的国产开源项目快速兴起，以填补我国在开源软件供应链各个环节的空白。然而，我国开源生态仍处在发展阶段，开源软件供应链渗透度与参与度不足，对开源软件供应链风险抵抗能力较弱。为此，建议发挥北京政策引领、科技与学术资源等优势，联合相关机构共同建立开源软件供应链支撑体系，保障我国开源生态健康发展，为数字经济和科技发展提供优质养料。



## 一、北京开源软件供应链存在问题

### 1. 开源软件供应链生态支撑不成熟。

目前，大量主流的开源软件多由国外基金会和社区主导，与诸多开发者、科技企业、研究机构、政府机构等共同组成成熟的开源生态，共享资源与信息。上述生态成员分布在开源软件供应链的各个环节，共同研究和应对开源软件供应链风险。我国目前也在构建由我国主导的开源基金会与开源联盟组织，加强开源生态的建设。然而相较于国外，我国的开

源生态起步较晚，在整个开源软件供应链中渗透和参与度低，导致对国外开源生态依赖较强，在开源软件供应链层面缺乏自主与主导能力。

2.开源软件供应链风险大但研究投入少。

根据中国科学院软件研究所相关研究表明，开源软件供应主要面临三大风险，即安全性风险、可维护性风险以及合规风险，为开源生态、信息化技术与科技产业发展埋下严重隐患。为应对上述风险，国外包括谷歌、微软、IBM、亚马逊、Linux 基金会、Apache 基金会等商业机构和基金会共同开展相关研究,并启动了诸如 OpenSSF、Sigstore、OpenChain 等相关项目，对开源软件供应链风险进行持续研究，并提供防控手段。相比之下，北京作为高科技产业与学术高地，对开源软件供应链风险的研究投入相对较少。

3.开源软件供应链风险评估标准与手段不足。

开源软件作为现代科技产业的重要组成部分，开源软件供应链的安全可靠至关重要。近年来，开源软件投毒、恶意删库、利用开源软件供应链漏洞的网络攻击等事件层出不穷。然而，目前尚缺乏开源软件供应链风险评估相关标准与手段。

## 二、北京发展开源软件的建议

1.发挥学术和技术资源优势,引导开展开源软件供应链风险发现与防控技术研究。

建议发挥北京学术与技术资源优势,联合在京的基础软件公司、互联网公司、开源软件公司、网络安全公司以及高校

和科研院所、国家信息安全漏洞库平台等核心单位，开展开源软件供应链风险发现与防控技术研究，为在京政府、企业、机构等提供安全、可靠、可持续的开源软件供应链保障。

2. 建立开源软件供应链风险评估标准与评估体系。

建议联合相关单位，从开源软件供应链安全性风险、可维护性风险以及合规风险角度出发，制定开源软件供应链风险评估标准，并建立包含评估工具、测评与认证在内的开源软件供应链风险评估体系，鼓励企业对其商业化软件产品进行开源软件供应链风险评估，以提升软件产品安全可靠性。

3. 建设开源软件供应链安全基础设施。

建设开源软件供应链安全公共基础设施，为在京的各类涉及开源的机构、企业、高校及研究院所提供包含开源软件供应链漏洞感知、开源软件关键节点识别、威胁监测、风险预警、风险评估等多种基础安全服务，降低各行业对开源软件供应链风险发现和处置成本并提升相关风险的应对能力，通过公共基础设施平台加速开源生态能力建设。

4. 进一步引导和推动相关行业参与并贡献开源。

鼓励和引导各行业在应用开源的同时，增加对开源的参与和贡献程度，尤其对于开源软件供应链中的关键节点，积极探索和掌握开源技术核心，并促进相关开源技术的迭代升级。对于掌握核心技术的开源社区与开源项目，可协助对接京内具有相关开源技术需求的企业，适当给与政策与资金支持，加速开源生态建设与开源技术成熟。