# PUBLIC SUBMISSION

**Docket:** NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and
Cybersecurity Supply Chain Risk Management

**Comment On:** NIST-2022-0001-0001
RFI-2022-03642

**Document:** NIST-2022-0001-DRAFT-0049
Comment on FR Doc # N/A

---

## Submitter Information

**Name:** Pe
**Addres**
**Email:**

---

## General Comment

The NIST Cybersecurity Framework would benefit from additional guidance related to robust C-SCRM
program development. Additional best practice guidelines would beneficially focus on continuous
monitoring requirements, mitigation practices, supplier cybersecurity guidelines, and auditing criteria for
self-assessment/improvement for C-SCRM programs at both government agencies and private sector
entities

# PUBLIC SUBMISSION

**Docket:** NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

**Comment On:** NIST-2022-0001-0001
RFI-2022-03642

**Document:** NIST-2022-0001-DRAFT-0050
Comment on FR Doc # N/A

---

## Submitter Information

**Name:** Pe
**Address:**
**Email:**

---

## General Comment

NIST's Cybersecurity Framework would benefit from more targeted supplemental information related to specific critical infrastructure sectors. While the general CSF is a solid foundation, the challenges facing each sector are unique for both the private sector and government. More targeted, sector-specific guidance within the CSF could articulate best practices informed by government-private sector partnerships and information sharing. Recommend aligning any sector-specific CSF guidance with existing schema of critical infrastructure and/or National Critical Functions.