

From: Lena Smart

Sent: Wednesday, February 23, 2022 7:48 AM

To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>

Subject: "RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management"

I have two recommendations for the NIST CSF update:

1. Include the SBOM requirement as part of the IDENTIFY bucket - if every Government Agency is going to ask for an SBOM then we should be measuring where we are with that request.
2. Somewhat tangential but along the same lines - SBOMs should be part of the FedRAMP SSP.

I would like to be part of any working groups you setup to work on the overhaul of the CSF, as I was part of the original workgroups in 2014 and very much enjoyed that collaboration.