Ke, Jessica - Intern

From: Friedman, Allan
Sent: Thursday, June 10, 2021 12:27 PM
To: SBOM_RFC
Subject: Fw: Comments from CISA contractor

From: VANDEWOUDE, MICHAEL (CTR) <michael.vandewoude@associates.hq.dhs.gov>
Sent: Wednesday, June 9, 2021 3:37 PM
To: Friedman, Allan <AFriedman@ntia.gov>
Subject: FW: Comments

Sorry to forward this to you, but the email address published in the Federal Register didn't work?

From: VANDEWOUDE, MICHAEL (CTR)
Sent: Wednesday, June 9, 2021 3:35 PM
To: SBOM_RFC@ntia.gov.
Subject: Comments

Hi, I am a contractor working with DHS Hq on C-SCRM. There is much to write about SBOM, but I'll be brief because these things are important and need to be addressed.

- I understand the EO is addressing Software, however, the SBOM should also address hardware, network and possibly services e.g., cloud and outsourcing. Components of hardware is as complex as software and vulnerabilities exist in the manufacturing of these products. This is also true of networks (especially with 5G around the corner).
- Data Fields – The number data fields is limited. There are third party suppliers who have 3rd party suppliers. Each should be listed with address and ownership. Anything built outside of the US should have a more detailed questionnaire.
- Workflow – Processes should be automated sequential automation i.e., from RFP/RFI issued by Procurement, responses should reviewed by Finance, Engineering (need to understand the impact to Infrastructure e.g., network, storage, change management and operations e.g., – what happens to the help desk and how do they support it

These are just high level thoughts. Recommend we build a RACI that shows Responsible, Accountable, Counseled and Informed. This will give agencies a guideline of structure.

Mike