PUBLIC SUBMISSION

As of: 4/25/22 12:28 PM
Received: April 21, 2022
Status: Pending_Post
Tracking No. l28-pzdg-xzwg
Comments Due: April 25, 2022
Submission Type: Web

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-0023
Comment on FR Doc # N/A

Submitter Information

Name: Colin Topping
Ad[redacted]
Email: [redacted]
Phone: [redacted]

General Comment

I work for a global Aerospace and Defence organisation where Supply Chain Risk Management is high up on the CISO's agenda and something I am directly engaged in with relation to Incident Management and Response. I'm also doing a part-time PhD that focusses on Supply Chain Cyber Security for critical infrastructure (CI). It is sponsored by the UK NCSC and relates to C-SCRM in general and Incident Management and Response in particular. I am also on the NCSC ICS/COI (Industrial Control Systems Community of Interest) that joins NCSC, regulators, academics, and industry together to develop best practice for securing ICS, specifically for CI. I am part of the Steering Group and a member of their newly formed expert group focused on Supply Chain.
My first paper focused on the C-SCRM advice offered to organisations from UK, US, EU national authorities, and to Water, Chemical, and Energy sector specific advice. It then looked at any standards or frameworks that were referenced and reviewed them to. The paper was published here. The main output from this research was the development of a C-SCRM taxonomy.

At the time, CISA was in its infancy, and it has done a lot of work to catch up. This is mainly with the ICS SCRM Task force and associated work groups. Added to that; NIST SP 800-161 Rev 1 (draft 2) forms a key component of my current paper (with a brief mention of how it is closely aligned to NIST SP 800-53 Rev 5 and the CSF). This contrasts global approaches for identifying and managing cybersecurity risks in supply chains. It looks at national authority advice from APAC, US, AND EU.
Abstract:
With the targeting of an increasingly complex and global supply chain by threat actors, we contrast the approaches of national authorities regarding the current threat landscape. We review their Cybersecurity Supply Chain Risk Management (C-SCRM) advice against our C-SCRM taxonomy, noting a diverse approach to the guidance offered. We saw NIST being increasingly signposted as being a freely available

and viable resource that organizations could adopt. NIST SP 800-161 aligns closely with the taxonomy, allowing for a complementary approach that lends itself towards becoming the pathway towards a common set of principles. Such a pathway would allow both businesses and suppliers the opportunity to deliver against an agreed common framework.

There are some areas of the taxonomy that aren't considered or addressed with the latest NIST C-SCRM output when comparing it to the taxonomy.
Extract:
When compared against the taxonomy, NIST SP 800-161 is broadly aligned, even down to the attribute level. There are some gaps that may be picked up by other NIST documents. The exclusion of suppliers is not directly considered. It does however point to adhering to legislative requirements, where this would be covered. Removal of a supplier is only touched upon deep down in the weeds of the document, and then only briefly. We believe that these areas are key components of C-SCRM and would benefit from being more obviously signposted.

To a lesser degree, there is also no consideration that service providers provide services to multiple customers, which may include direct competitors. This can introduce separation of duties requirements to be contracted. Additionally, the business priorities of public and private organizations are likely to be very different and building that awareness within the document would promote a greater appreciation of that potential dichotomy.

Attachments

NIST C-SCRM RFI

C-SCRM

Beware Suppliers