PUBLIC SUBMISSION

As of: 2/28/22 10:47 AM
Received: February 23, 2022
Status: Pending_Post
Tracking No. l00-al3y-8xuj
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-0003
Comment on FR Doc # N/A

Submitter Information

Organization: Sullivan Wright Technologies

General Comment

The NIST Cybersecurity Framework has been a helpful document for us in securing our small business clients. The control structure has been easy to adapt to the needs of small businesses. Using this document as an authoritative reference has also helped convey the importance of the different security controls and measures to non-technical and non-risk management personnel. We have used the CSF along with the CIS Controls to develop our own, simpler, set of controls that we can use in our clients who have no other compliance requirement. It's not just me saying these are good ideas, but I'm backed up by a trusted source. I hope you will continue to maintain and update the CSF as the security landscape changes. I'm extremely happy to have this document as well as the extensive library provided by NIST to support my company in securing our small business clients.

My only suggested additions would be the two measures/controls that we add that have no formal reference:
- That all IT infrastructure is actively managed by a qualified internal or outsourced staff
- That the organization procures adequate cyber liability or data breach insurance and/or retains cyber crime knowledgeable legal counsel

The first bullet is assumed in most larger organizations, but cannot be assumed in the smallest ones. Many of these small organizations cobble IT assets together from local stores without any formal management or design. I've found that it's impossible to secure an organization without some sort of active and qualified IT management in place. As a security consultant, I need an IT team to implement and manage many of the security measures I recommend.

The second bullet seems to be a new area of focus and may not be comfortable for the US government to advise, but we advise it in all clients. With the right policy, much of the response and recovery effort can be covered where as without the policy the company will be on their own and may not be able to afford the cleanup effort. We are a small company that supports other small companies in a small state so

bringing in outside IR and forensics teams is cost prohibitive for even our largest clients. Insurance would bear that burden for them and often do a better job at recovering from large breaches than we could.

I can't thank NIST enough for all the great work, though. Please keep doing what you are doing. It's appreciated by the little guys in the trenches.