From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] NIST 800-171 Comment: Updating Section 2.1 or Adding Security Requirement(s)
Date:	Friday, September 16, 2022 2:53:59 PM

Hi NIST,

Below are some comments on updating section 2.1 or adding a Security Requirement to NIST 800-171.

Please don't hesitate to reach out if you have any questions.

Background:

While attending the CMMC Day on May 15th, I had a chance to hear Victoria Pillitteri speak. During her talk, she said that when the NIST 800-171 requirements were being developed, NIST assumed that companies implementing NIST 800-171 would have policies in place to support the NIST 800-171 requirements.

For better or for worse, stakeholders only want to implement what's in NIST 800-171 and they also have too many competing priorities that prevent them from attending industry events to hear about the assumptions NIST used to create NIST 800-171. This is especially the case, when it comes to executive sponsors that are paying for their companies NIST 800-171 program.

Recommended Change:

Below are two options for increasing transparency about the assumption NIST made on companies having policies in place to implement the NIST 800-171 Requirements. These changes will provide clarity to all non-federal organizations, that need to implement NIST 800-171.

Option 1

Update NIST 800-171 Section 2.1, to include the assumption that non-federal organizations have policies in place to support the implementation of NIST 800-171 Security Requirements.

Option 2

Add a new Security Requirement to NIST 800-171, that requires the development and maintenance of policies to support the implementation of the NIST 800-171 Security Requirements. You could implement this option in one of two ways. First, you could create a single Security Requirement that requires the development and maintenance of a policy for all of the Security Requirements. Alternatively, you could take a NIST 800-53 approach, where there would be 14 Security Requirements, 1 Policy Requirement for each of the 14 security requirement families in NIST 800-171.

Cheers,

Andrew Freund
Founder & CEO
[redacted]

[redacted]