From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Wednesday, July 5, 2023 9:36:10 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

I did not use the template for this comment as it is not on one specific requirement, but on something which is utilized in multiple requirements.

Organizational Defined Parameters (ODP)

There are several different types of ODPs in the draft of revision three, these include, but are not limited to:
Authorities, Policies, Procedures, Personnel or roles, Security functions, Time period, Numbers, Conditions or trigger events, Controls, Types of external systems, Frequency, Events / event types.

Certain ODP definitions would create issues due to the difference in size and organization of the defining organization and SMB which protect the organization's information. Among these are: Authorities, Policies, Procedures, Personnel or roles, Security functions.

As an example, the defining organization may call for a role of Chief Privacy Officer. Smaller organizations may not have heard of this concept previously, let alone have a CPO or equivalent in their organization. Similarly, these other ODPs could be defined in ways which are unknown to the contractor, or do not align with their business model.

The assignment statements for requirements with these parameters should not be ODPs, rather they should be left for the company implementing 171 to define.

John Perreault
Prin Security Engineer
Information Technology | Corporate

Mercury Systems
[redacted]

[redacted] | **mrcy.com**

The contents of this email and any attachments are intended only for the designated recipient(s) and may contain proprietary information of Mercury Systems, Inc If you received this email in error, please contact the sender and delete the material from your systems