From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] Comments for Revision 3
Date: Thursday, September 15, 2022 9:54:28 AM
Importance: High

NIST,

In response to the call for comments, please see below.

Comments for consideration of Revision 3 from SoundWay Consulting, Inc.

Arguably the single greatest challenge for NIST is the fact the US Government does not want to tell industry how to do things, yet Industry desperately wants to be instructed "exactly how to achieve the goals and objectives" of each prescribed control. SoundWay's team members have performed over twenty-five assessments of Government Contractors measured against versions 1 and 2. The following comments are a direct result of these lessons learned.

1. The US Government's presumption that corporate Americana operates with corporate policies and subordinate procedures for managing cyber risk is categorically erroneous. Materials that are within an Index of a Special Publication are rarely assessed against, even if a Federal System. The Government is justified in amending its presumption to "require" formal corporate policies as part of revision three so as to align with the -1 controls from NIST SP:800-53r5.
2. NIST Should strongly consider an abridged version of SP:800-171 exclusively for organization that need to "Protect Federal Contract Information in Non-Federal Systems and Organizations". By doing so, the following benefits will occur:
   A. Reduce confusion by industry when demonstrating conformance against only 17 of the 110 controls from revision 2 and on behalf of Government to reduce conflicting contract clauses.
   B. Assist the Department of Defense and other Departments and Agencies to construct SPRS scoring mechanisms that are currently being wrongly scored by industry because they legitimately can state "we do not have CUI" therefore, no point deduction for at least 19 controls using the current DOD scoring methodology.
3. With the developments of CSPs like Microsoft's GCC-HIGH environment, NIST Should have "implicit" guidance on defining common controls so third-party assessments can be more effective and efficient and thereby lower costs of ownership.
4. Currently in 3.1.4 (b) is written as, "responsibilities for duties that require separation are assigned to separate individuals: and". This is grossly incomplete. SoundWay is seeing on numerous occasions where guidance by industry interprets this obligation merely as "any" person versus a "qualified person". Having somebody in Human Resources provide oversight to IT adds zero value. By defining a "qualified person", the Government can impose obligations that stipulate:
   A. An individual with no less than two years of security practitioner experience
   B. Possesses a professional certification like CISSP, CCP, etc.
   C. Role is not subordinate to IT Operations
   D. Ensure the intent of the control and objective is met by using resources that are aligned with the responsibility
5. 3.11.1 Risk Assessments currently reads as "Periodically assess the risk to organizations (including mission, function, image, or reputation)….." Revision 3 should also include "financial impacts". As 800-171 is really designed for Government Contractors, NIST would be remiss by not understanding that a cybersecurity incident has significant financial impacts that could either force the operations out of business or significantly hamper cost, schedule, and performance of a government contract. By including financial aspects of the risk assessment, the organization in question will need to capture

these risks and also identify if the risks are acceptable or is there a means to transfer the risk to a third-party mechanism like a cyber liability insurance policy that covers first and third-party damages.

Respectfully,

Carter

Carter Schoenberg, CISSP & CMMC-RP
Vice President – Cybersecurity Solutions & Chief Cybersecurity Officer
SoundWay Consulting, Inc.
[redacted]
www.soundwayconsulting.com
[redacted]