Comments on 800-171B

HC

Hirsch, Corey <Corey.Hirsch@Teledyne.com>

Tue 7/16, 3:08 PM

sec-cert

171B IPD Public Comment

I wish to offer these comments regarding the proposed 800-171B controls:

The following proposed enhanced security requirements introduce risks that exceed potential benefits, and should not be approved / included as currently drafted:

3.13.2e Introducing randomness effects authorized and unauthorized system users similarly. Purposefully disrupting the smooth operation of the network will introduce new risks for product non-conformance, potentially creating safety risks for users downstream. Since Advanced Persistent Threat actors most often are acting as privileged users, establishing these 'landmines' for them also establish the potential for detonation against actual authorized privileged users. While some of these techniques MAY be appropriate in certain organizations under certain circumstances, requiring their application across the board would be value-destroying (i.e. the damages inflicted would exceed the benefits realized).

3.13.3e Similar to 3.13.2, these tactics carry additional separate risks for infliction of accidental operational disruption that will likely often exceed any benefits arising from confusion of APT actors. Such tactics should be optional, for employment in select organizations and specific circumstances where the benefits might be high, and the risks relatively low. It would be unfortunate to mandate such tactics with a broad brush. This document appears focused primarily on prevention of Confidentiality and Integrity losses. There is an important third component, Availability, and controls such as this one pose operational risk in that area.

With best regards,

Dr. Corey Hirsch, CISO
Teledyne Technologies Incorporated