[redacted]

From: Gould, Evan (HII-Mission Technologies) [redacted]
Date: Thursday, September 8, 2022 at 10:35:04 AM UTC-4
Subject: Pre-Draft Call for Comments on the CUI Series
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

The requirement to "Limit system access to …devices" is potentially very restrictive depending on its interpretation. Was the intent to prohibit access to CUI Basic (at a minimum) from any device unless that device is specifically approved (i.e., the risk is accepted)? It seems that that was NOT the intent since such as requirement was included in 800-172 (3.1.2e). Given the proliferation of web-based access from non-company-issued devices, for example, this can be very restrictive if strictly interpreted. Seeking clarification of intent (and hoping such clarification will be included in the Discussion or Supplemental Guidance of the control). If the intent is to prohibit personally owned devices from accessing CUI, please state that explicitly.

3.3.3 Review and update logged events.

The title of this control continues to mislead. The Discussion for this control says, "The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged." However, the title does not reflect that intent, and continues to be interpreted as "Review the log files." Recommend rephrasing for clarity.

3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

Similar to comment for 3.1.1. The requirement to "Authenticate (or verify) …devices, as a prerequisite to allowing access to organizational systems" is potentially very restrictive. Unless personally owned devices are outright prohibited from accessing CUI, authenticating personal devices (rather than authenticating the user using the device) is a burden to implement that is not commensurate with the security benefit gained. The Discussion text does not mention device authentication except to say that "Device authenticators include certificates and passwords"

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

"Minimum password complexity" is no longer in alignment with SP 800-63 guidance on Memorized Secrets.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

What technical or operational mechanism can be implemented to meet this control? It remains unclear. The Discussion says, "This requirement prevents information produced by the actions of prior users or roles …from being available to any current users or roles …that obtain access to shared system resources [(e.g., registers, cache memory, main memory, hard disks)] after those resources have been released back to the system." Memory management is performed by the operating system (Windows and Linux) and by the applications and services installed. Explicit examples of solutions or approaches would help greatly.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

The increasing use of GovCloud-based enterprise functions and a growing remote workforce decreases the relevance of this requirement. For example, enterprises that use Microsoft's GovCloud- based Exchange, SharePoint, OneDrive etc. may choose to allow split-tunneling (from company-issued laptops) so that network traffic can go directly to the cloud services without going through a central company datacenter via VPN. If such an alternative is a risk-based decisions, please state so explicitly in the Discussion

Evan Gould

Cybersecurity Lead

Cloud Center of Excellence (CCoE)

HII Mission Technologies

Upcoming Out of Office:

None

Tel: [redacted] (Eastern) | email: [redacted]

Confidentiality Statement:

HUNTINGTON INGALLS INDUSTRIES PROPRIETARY – This e-mail contains information proprietary or private to Huntington Ingalls Industries, Inc., and is not to be disclosed to, copied by, or used in any manner by others without the prior express, written permission. If you are not the intended recipient, please delete without copying and kindly advise the sender by e-mail of the mistake in delivery.