From:	800-171comments@list.nist.gov on behalf of [redacted]
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comments on NIST SP 800-171r3 initial public draft - 3.4.1 Configuration Management: Baseline Configuration
Date:	Wednesday, January 24, 2024 11:51:24 AM
Attachments:	sp800-171r3-fpd-comment-template.xlsx
Importance:	Low

3.4.1 Configuration Management: Baseline Configuration

Baseline configurations continues to be a source of confusion. Doing the following will alleviate this confusion and more generally standardized baselines across organizations because they better understand the expectations. This change would permit IT organizations to better understand what a System is and what is in scope. It also defines the software which require a security baseline and what controls are expected to be addressed in the baseline. This is a common contention point between GRC and IT.

1) It needs to be made clear that minimum security baseline configurations must be developed for all systems in scope of CUI.
2) Clarify the scope of the security baselines i.e., do we mean just device operating systems or do we also me applications that "have an IP address assigned".
3) Specify the specific control minimum NIST 171 control requirements that should be addressed in the baseline control guidance. This enables implementers understand the controls to be considered. Specify that this aligns with the 171 Moderate control requirements. 172 should have something similar for the High control requirements.
4) If appropriate, consider referencing the disablement of unnecessary ports, protocols, and services in the guidance; if possible with common examples.
5) If possible, provide source and guidance for existing security baselines that may be tailored to organizational needs.

Comment #	Submitted By (Name/Org): *	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Ryan Speight	Technical	NIST 800-171R3 Final Public Draft	22	769	3.4.1 Configuration Management: Baseline Configuration Baseline configurations continues to be a source of confusion. Doing the following will alleviate this confusion and more generally standardized baselines across organizations because they better understand the expectations. This change would permit IT organizations to better understand what a System is and what is in scope. It also defines the software which require a security baseline and what controls are expected to be addressed in the baseline. This is a common contention point between GRC and IT.	1) It needs to be made clear that minimum security baseline configurations must be developed for all systems in scope of CUI. 2) Clarify the scope of the security baselines i.e., do we mean just device operating systems or do we also me applications that "have an IP address assigned". 3) Specify the specific control minimum NIST 171 control requirements that should be addressed in the baseline control guidance. This enables implementers understand the controls to be considered. Specify that this aligns with the 171 Moderate control requirements. 172 should have something similar for the High control requirements. 4) If appropriate, consider referencing the disablement of unnecessary ports, protocols, and services in the guidance; if possible with common examples. 5) If possible, provide source and guidance for existing security baselines that may be tailored to organizational needs.