From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on NIST SP 800-171r3 initial public draft
Date: Friday, July 14, 2023 6:55:05 PM
Attachments: NIST Comments.2023-07-14.xlsx

July 14, 2023

TO NIST:

Please find attached comments from the Department of Justice regarding the National Institute of Standards and Technology (NIST) draft publication titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" (NIST SP 800-171r3).

Thanks,

Eric Gormsen
Office of Legal Policy
Department of Justice

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	DOJ CIV-Fraud	Technical	Defense Federal Acquisition Regulation Supplement, 252.204-7019 and 252.204-7020	45	1681	We suggest that control 3.12.2 ("Plan of Action and Milestones") require organizations to provide a date when the POAMs will be completed and a score of 110 will be achieved. Requiring a date for implementation of all requirements serves two purposes. First, it ensures that the organization devotes resources to remediating the POAMs by its deadline. Second, it provides an agency considering a contract with an organization information regarding the timeframe for remediation of deficiencies. For example, an agency may be willing to accept a deficiency that will be remediated within one month, but not a deficiency that will be outstanding for six months or longer. Including this language would be consistent with the requirements in the Defense Federal Acquisition Regulation Supplement, 252.204-7019 and 252.204-7020.	Add new clause: "c. Provide the date that a score of 110 is expected to be achieved."
2	DOJ-EOIR	Technical	NIST SP 800-171r3	20	722	Is the requirement for an authoritative time source for time stamps no longer applicable?	Seeking clarification.
3	DOJ-EOIR	Technical	NIST SP 800-171r3	21	766	What does “most restrictive mode consistent with operational requirements” mean? STIG hardening guide? Another hardening guide?	Seeking clarification.
4	DOJ-EOIR	Technical	NIST SP 800-171r3	32	1206	it appears we may need additional training resources to do incident response correctly. Any recommendations?	Seeking clarification.
5	DOJ-EOIR	Technical	NIST SP 800-171r3	38	1412	Need futher clarification on how specific these checks must be. How do you measure stability? How do you measure reliability?	Seeking clarification.
6	DOJ-EOIR	Technical	NIST SP 800-171r3	52	1972	Does DNS filtering services suffice for this requirement?	Seeking clarification.
7	DOJ	General		4	79	ODPs would appear to introduce variation that could defeat the purpose of having a streamlined set of requirements or minimum cybersecurity standards. They also may potentially result in variances across contractors that may be difficult to track.	We suggest that NIST: (1) eliminate or reduce the introduction of ODPs; (2) if maintaining ODPs, provide default values that organizations can use without the burden of creating specific ODPs; and/or (3) set outer bounds on the acceptable parameters for organizations to use.