From:	"Jeffrey Myers" via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] NIST 800-171 Rev 3 comments
Date:	Friday, June 23, 2023 11:10:32 AM
Attachments:	image001.png sp800-171r3-Aptima Comments.xlsx

Included are comments for the NIST 800-171 Revision 3

Jeff Myers
Title: Compliance and Cybersecurity Team Lead
[redacted]

APTIMA, Inc. | **www.aptima.com**
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Aptima Inc.	Technical	NIST SP 800-171 Rev3	24	895	By requiring companies to operate on a purely Whitelist of approved software, this implication will stiffen and delay adaptation of new and emerging technologies to buisnesses. This ability to adapt and incorporate new technoligies allows private and public companies to continually create products with the best technology has to offer.	Require companies to maintain a list of both approved and unapproved software, but not force an Allow by Exception requirement. Stress the importance of software scanning, and vetting before use. This allows the companies to rely on their risk acceptance level to determine the switfness of accepting new software components.
2	Aptima Inc.	General	NIST SP 800-171 Rev3	59	2250	By applying an adequate SCRM statretgy all components of a system must be evaluated down to the smallest degree. Requiring an extensive amount of overhead to be applied to each purchase made. This is a terribly cost prohibitive action for small and medium sized buisness to account for.	Require companies to maintain a list of unapproved vendors or manufacturers based on available information provided by security agencies. In addition maintain an active hardware inventory that is able to be searched when new information is release on bad components or suppliers.
3	Aptima Inc.	Editorial	NIST SP 800-171 Rev3	46	1730	Define "exchange" of information better.	N/A
4	Aptima Inc.	General	NIST SP 800-171 Rev3	46	1730	How does this differ from Contract language between Subs and Primes to address flow down requirements bassed on directives and requirements in contract language.	Annotate in the control that this would apply to contracts that don't include flow down controls already (EX: DFARS 7012 clause requirements)
5	Aptima Inc.	General	NIST SP 800-171 Rev3	46	1730	If utilizing products or tools from an organization (Microsoft) that are based on Cloud Models and have been vetted with other C3PAO's do this still require a written MOU/SLA.	Annotate in the control that the acceptance of Shared Responsibilities from products that have been formally vetted and approved by a certified C3PAO for use in the FedRAMP MarketPlace (or similar) do not require additional MOU's/SLA's
6	Aptima Inc.	Technical	NIST SP 800-171 Rev3	58	2199	What is the scope of "system component"	Add language to define system components that do not pose a security risk or a risk assessment has been conducted to alievatiate the potential of risk, no required under this control

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*