From: [redacted] via 800-171comments
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] NIST 800-171 Rev 3 Draft 1 Comments
Date: Friday, July 14, 2023 2:53:15 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png
image008.png
image009.png
sp800-171r3-ipd-comment-Win-Tech.xlsx

Hello!

Please see attached for comments from Win-Tech (a SMB manufacturer).

Thank you for y'all's time collecting these and reviewing!

Have a good weekend,

--

Allison K. Giddens
Win-Tech, Inc.
AS9100 Certified, Veteran-Owned

[redacted]
[redacted]
www.win-tech.net
[redacted]

Win-Tech Office Hours: 7:00am-5:30pm (Monday-Thursday) and closed on Fridays.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
	Win-Tech Inc.	Editorial/Technical	NIST SP 800-171r3 ipd	15	79	NIST not being part of the regulatory ecosystem creates problems within industry where expectations are not managed and/or tailoring becomes unsupportable and unsustainable.	NIST needs to take accountability in the ecosystem in which their guidelines and standards are utilized to help with understanding cost to implement and maintain as well as repercussions of the standards and how they may be tailored to non-Federal agencies.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	21	783	**3.4.2 Configuration Settings (reference to ODP)** - ODPs define common secure configurations. This opens up agencies to add to the regulatory requirement (which DoD is prone to do). Requirements of Prime Contractors are not necessarily requirements of subcontractors. Lower tiers would be subject for what the higher tiers are subject to. Depending on the STIG if it becomes part of the ODP there could be a tremendous amount of burden to SMB.	Remove ODPs or clarify which tiers are responsible for meeting. Since CUI at the start of a contract is not necessarily the same CUI further down the supply chain this flow-down becomes overkill and "noise" to those not necessarily needing it. Leaving as-is (applicable to everyone responsible for meeting NIST 800-171) does not contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	24	895	**3.4.8 Authorized Software -** Allow by Exception - blacklisting is no longer allowed only whitelisting. In a SMB environment particularly a small manufacturer or job shop with many customers across many industries working in an enterprise environment this is extremely burdensome and would lead to significant productivity impact. Implementing an "Allow List" only is a large impact for small businesses that will require on-boarding more technical implementations. If resources are ava lable for this setup can be relatively easy but maintenance – especially in a SMB environment – is not.	Allow blacklisting. Allow-listing does not contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	27	1025	**3.5.3 MFA** - Multifactor authentication for all access can be costly and cumbersome in a SMB environment. Additionally not all software supports MFA.	Allow for exceptions to MFA referencing other ways to mitigate risk when software or application is otherwise compliant.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	29	1069	**3.5.7 Password Management (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define composition and complexity rules – What if system cannot support? Microsoft only enforces 8 characters in Azure AD.** The ODP variability is difficult to standardize f multiple customers enforce different parameters.	Remove ODP. Certain systems cannot support specific composition/complexity rules and that doesn't mean the data is less secure (especia ly when other controls are met such as MFA).
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	31	1171	**3.6.2 Incident Monitoring, Reporting, and Response Assistance (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define who you report to – Reporting comes from higher regulations (DFARS, etc), allowing customer to define gets unruly when working with multiple customers with varying options on who needs to be informed.** The ODP variabi ity is difficult to standardize if multiple customers enforce different parameters.	Remove ODP. Adding specifics (when agencies already require this) does not contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	36	1351	**3.8.5 Media Protection** was encrypt OR physica ly protect. Now the updated requirement is "encrypt AND physically protect." This is overkill.	Allow for encryption OR physical protection. Requiring both does not contribute towards the goal of supporting confidentiality of data anymore than one by itself.
	Win-Tech Inc.	Editorial	NIST SP 800-171r3 ipd	39	1457	**3.9.3 External Personnel Security/3.16.3 External System Services** – "external providers" "external system service" – NIST should formally define these terms in the Glossary. This is an important definition as other entities have competing definitions and will certainly impact industry going forward.	Formally define terms in Glossary. In order to support the confidentia ity of data government agencies MUST use a standardized definition instead of being left to their own devices to come up with their own definition. Businesses don't operate in vacuums with only one agency. If one agency defines an MSP differently than another this actually does the goal of confidentiality of data disservice.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	50	1457	Requiring external personnel especially cloud services to comply with an SMB's security policies and procedures as well as monitoring that compliance is unrealistic.	Redefine this requirement to differentiate the types of roles that would be required for these vs just stating a l external providers. Requiring this does not contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	53	2010	**3.14.1 Flaw Remediation - (reference to ODP)** - In section "c" - the ODP related to the time allowed to install security-relevant software and firmware updates is problematic. SMBs manufacturing facilities may need to take production down or manage this during planned maintenance which could fall beyond the ODP parameters.	Remove ODP or defer parameters to suggested timeline per software recommendations (based on identified flaws urgency etc.). There is not a way to standardize this and it contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	56	2127	**3.15.1 Policy and Procedures (reference to ODP) - ODPs define how often CUI policy and procedures need to be reviewed and updated.** ODP infringes upon contractor's Corporate policies and procedures.	Where a timeline is mentioned in review of policies/procedures- the ODP should be set at contractor's existing frequency. Overriding this does not contribute towards the goal of supporting confidentiality of data.
	Win-Tech Inc.	Editorial	NIST SP 800-171r3 ipd	56	2114	**3.14.8 Spam** - Control is irrelevant to protection of CUI.	Remove control spam is an annoyance but not a direct threat to the confidentiality of CUI.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	58	2199	**3.16.2 Unsupported System Components** - requiring unsupported systems to be replaced is extremely burdensome to SMB. In a manufacturing environment many machines costing hundreds of thousands of dollars may not "talk" to the latest Operating Systems but are machines producing validated and conforming quality product.	There are other measures to consider to mitigating these risks. Remove the requirement to replace unsupported systems or include risk mitigation requirements to allow for unsupported sytems.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	59	2224	**3.16.3 External System Services (reference to ODP): ODP is specific to implementation and seemingly do not provide value as long as there is compliance with the control. ODPs define what controls, processes, methods and techniques are implemented - What if different agencies want different things? There can be no consistency to this.** The ODP variability is difficult to standardize if multiple customers enforce different parameters.	NIST should publish a baseline for the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed or when operating system introduces limitations but others meets compliance requirements.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	59	3.16.3	**3.16.3 External System Services (reference to ODP)** – ODPs define controls – Customer could require compliance with a variety of competing regulations. The intent to lower risk could actually introduce more risk by reducing the amount of vendors available willing and compliant.	Clarify which tiers are responsible for meeting. Define ESP MSP CSP (recognizing they are not all equal and perform different roles in the environment). Not defining these increases risk of confidentiality of data because companies will be defined differently across different projects and partnerships.
	Win-Tech Inc.	Technical	NIST SP 800-171r3 ipd	59	2251	**3.17-1-4 Supply Chain -** It's unclear whether a SCRM is needed for all systems with a corporation or just the systems processing CUI.	SCRM should only apply to the systems processing storing or transmitting CUI.
	Win-Tech Inc.	General	NIST SP 800-171r3 ipd			Understanding how agencies or the customer is going to define the 112 ODPs would need to be made a part of the RFI/RFP process. Large businesses have an advantage as they are more equipped to handle the implementation and interpretation of potentially varying ODPs. Small business would need to have expanded resources available to them (to be flexible enough to adjust/evolve set ODPs) in order to be competitive.	**NIST should publish a baseline for the standard** in lieu of the ODPs that should be used for the majority of contracts with modifications only being required on specific instances where additional security is needed or when operating system introduces limitations but others meets compliance requirements. (where a time ine is mentioned - annually should be set as the baseline) Where there is low-risk or a baseline is inconsequential but still needs definition the contractor should be able to define.
	Win-Tech Inc.	General	NIST SP 800-171r3 ipd			Removal of enduring exceptions was not addressed.	Add a section discussing enduring exceptions and how they would now be handled in the new revision as well as adding some additional context in the FAQ.
	Win-Tech Inc.	General	NIST SP 800-171r3 ipd			The addition of Planning (PL) System and Services Acquisition (SA) and Supply Chain Risk Management (SR) will require review evaluation and implementation. This is burdensome on SMB many of which are subtiers but will be required to be compliant with the new revision of NIST 800-171.	Offer ranges for implementation or set basic/low threshold minimum actions to be taken for subtiers.
	Win-Tech Inc.	General	NIST SP 800-171r3 ipd			171 by nature of its alignment with 53 seems to only target classic IT architecture and does not align with emerging models like those in SMB where CUI primarily lives in a SaaS tool and is pulled to employee laptops who are working remotely and not on a corporate network.	Account for more modern architecture that's used in SMB (and larger companies). Similarly relating this to defined terms (MSP CSP etc) will help decrease the risk of loss of confidentiality of data.