Dear NIST CUI Series team:

A few brief comments related to the pre-draft request for comments on the NIST controlled unclassified information series:

NIST should review and account for the fact that many organizations and agencies are using the CUI series (especially SP 800-171 and SP 800-171A, also increasingly SP 800-172 and SP 800-172A) as a core reference point for eligibility for access to information necessary to do business with the government and/or major contractors. This is also a) a positive development (in terms of overall information security) and b) a significant technical and implementation challenge and hurdle, especially for smaller, disadvantaged and/or our most innovative firms.

In its revisions, we STRONGLY recommend that NIST take into consideration how its series is being referenced and utilized across the government contracting enterprise, and work with large contractors, contracting agencies and smaller and midsize firms (as well as with technical assistance providers including Manufacturing Extension Partnership Centers, Procurement Technical Assistance Centers, Small Business Development Centers, Partnership Intermediaries, and Regional Innovation Cluster organizations as well as relevant industry associations) to identify, understand and integrate the key issues and addendums/clarifications that may make the CUI series more user-friendly and accessible. This type of proactive engagement will help to ease the cost of implementation where possible for organizations across the board.

Along these lines, we recommend the NIST CUI Series team integrate use cases for cloud-based architecture and applications into the principles and examples outlined in the SP 800-171 and (where applicable) SP 800-172 series. Many organizations are transitioning to this type of architecture and outlining how it might be implemented properly and securely from a system architecture and risk management design perspective would be useful.

Please also consider that many smaller organizations (especially non IT-centric organizations such as manufacturers) rely heavily upon 3rd-party hosting, management and support of core information systems and resources. Adjustments to the use cases and guidance relative to how to manage and interface with 3rd party resources (including reference to shared responsibility models and other modes of assigning responsibility for various functions to the appropriate resource(s) while maintaining oversight of core policies and procedures in the main business are important to consider.

If NIST CUI team can review baseline assumptions (including information currently included in the appendices to NIST 800-171) and determine whether certain aspects of those assumptions should be called out more formally in the guidance, that would be helpful for many organizations that are "new" to this framework to understand more fully the task at

hand before them and how their current system(s) and processes fit with the baselines outlined in the "medium security" aspects of SP 800-171.

Thank you for the opportunity to comment and we stand ready to provide additional information and input from our perspective as technical assistance providers and supporters of both manufacturers and third party service providers trying to work through these issues and collectively improve our nation's information security and risk management posture.

Thank you,

The FloridaMakes team

--

Michael Aller
Director, Supplier Development
FloridaMakes
201 East Pine Street, Suite 735
Orlando, FL 32801
Main: ▮▮▮▮▮▮▮ | **Cell:** ▮▮▮▮▮▮▮
www.floridamakes.com