New Mexico State University
Comments regarding review of **NIST SP 800-171B** – Comments Due August 2, 2019

As the NMSU system Chief Privacy Officer and IT Compliance Officer, I have reviewed the draft NIST SP 800-171B publication and have no edits and/or comments to the draft publication other than congratulating the authors for focusing the enhanced security requirements on APT. Additionally, the posture of scope applicability and making it applicable only when mandated by a federal agency in a contract, grant or other agreement is very appropriate. This posture provides an opportunity to Universities to negotiate dedicating a portion of the funding to meet the added security requirements. Overall, good job and I have provided below copies of the relevant sections within the publication, which are relevant and therefore support my overall comment(s).

Advanced Persistent Threat (APT).

CUI ENHANCED SECURITY REQUIREMENTS

The enhanced security requirements are only *applicable* for a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement.

The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry [NARA CUI].

In certain situations, CUI may be contained in a critical program or a high value asset.[6] These critical programs and high value assets are potential targets for the advanced persistent threat (APT).

The enhanced security requirements apply *only* to components[10] of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components when the designated CUI is contained in a critical program or high value asset. Additionally, the enhanced security requirements address protecting the integrity of CUI by promoting: (1) penetration resistant architecture; (2) damage limiting operations; and (3) designing for cyber resiliency and survivability.

Nonfederal organizations may elect to specify and implement requirements in this appendix (or elements thereof) based on mission or business needs, criticality analyses, and risk assessments.

LIMITING THE SCOPE OF THE ENHANCED SECURITY REQUIREMENTS

The *enhanced* security requirements in this chapter are only applicable for a nonfederal system or organization when mandated by a federal agency in a contract, grant, or other agreement. The requirements apply *only* to the components of nonfederal systems that process, store, or transmit CUI contained in a critical program or high value asset or that provide protection for such components. The nature of critical programs and high value assets is such that they are likely to attract attention from the Advanced Persistent Threat (APT), and therefore, warrant the additional protection and cost that are associated with the enhanced security requirements.