August 2, 2019

Re: Draft NIST Special Publication (SP) 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets.

To whom it may concern:

The University of Southern California respectfully submits this letter as a response to the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) proposal, outlining enhanced security recommendations to protect Controlled Unclassified Information (CUI) for nonfederal systems and organizations where information runs a higher than usual risk of exposure. From a university perspective, we greatly appreciate a public comment period to allow for the thorough exchange of information, insights, as well as, allowing the government to properly assess how a change – to any number of the 32 recommended enhanced security requirements – may directly impact certain academic and scientific communities. However, a 30-day comment period is insufficient for a document of this scope and complexity; an extension is needed for our members to review and provide substantive comments.

As an institution, we recognize the real need to ensure that U.S. national security interests around protecting CUI in nonfederal systems and organizations – like many Information Sciences Institute – priorities including artificial intelligence, networking and cybersecurity, and quantum computing are identified and accounted for.

Draft NIST SP 800-171B is intended to apply to a contract-by-contract basis for critical programs with the costs to implement and maintain these additional protections typically allowable contract cost by the government. However, a case-by-case approach will be problematic; unlike CUI registry with its well-defined categories the threat-centric approach appears subjective and *ad hoc*. It also appears inconsistent with the National Archives and Records Administration guidance that agencies may not implement safeguarding or dissemination controls other than those permitted by the CUI program

Additionally, the costs are prohibitive, with estimates ranging up to $46 million. For large defense contractors that routinely manage critical programs or high value assets these costs may be justifiable; for universities that may occasionally receive such designations on an individual contract or agreement basis the costs cannot be justified.

The criteria and basis for designation need to be more clearly specified, as well as, whether agency designations will be pursuant to the Department of Homeland Security program for high value asset identification established by Office of Management and Budget Memo M-19-03. However, that program applies only to Federal information systems.

Having two sets of security requirements for CUI is unduly burdensome and bureaucratic and likely to lead to confusion.

Restricting access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization proves problematic if an individual is part of the data supply chain where there will be upstream and downstream data sources or destinations.

The enhanced requirements violate the letter and spirit of NSDD-189 and are inappropriate for use with fundamental university research, which should be clearly stated.

While the guidance refers to equally effective alternative measures, it would be useful to see specific examples and to provide guidance on how that equivalent effectiveness may be determined.

Unless it is mandated for agencies to state applicability in funding announcements, this has the potential to impose huge administrative burden when an awardee learns of requirements only at the time of contract. Additionally, it may be impossible to comply within a timeframe that meets government contractual needs.

Through the comment process, we hope our thoughtful response, along with that of other institutions, provides Commerce and other agencies information that can be used to update DRAFT NIST SP 800-171B to meaningfully protect national security interests while maintaining a strong level of U.S. commercial viability and competitiveness and supporting a thriving basic research program at U.S. institutions of higher education.

Sincerely,

Douglas Shook, Ph.D.
Chief Information Officer
Vice Provost
Professor of Data Sciences
University of Southern California

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
1	University of Southern California Information Sciences Institute	Eileen Lu	G	20	659	674	3.6.1e	the cost of forming SOC is an organization change that will involve leadership and human resource as well as consitent budget to to sustain the existence of such center. While the cost consideration is calculated in the Cost Reference file https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf, we are concerned that it's way under estimated. ($150k-1M) since it's not just one time cost.	
2	University of Southern California Information Sciences Institute	Eileen Lu	G	20	678	692	3.6.2e	the cost of forming CIRT is an organization change that will involve leadership and human resource as well as consitent budget to to sustain the existence of such center. There is not cost estimate information posted in Cost Reference file https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf. and if it is considered cost under SOC, again, we are concerned that its way under estimated since it will not just be one time cost.	

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
3	University of Southern California Information Sciences Institute	Eileen Lu	E	12	471	482	3.1.1e	in a general IT environment, it would be extremely difficult to implement tools as suggested in the verbiage (dual authorization for the execution of priviledged commands). However, this could be interpreted into just general operation and approval process that needs to be in place instead of providing technical tool/software to ensure approval exist before actual commands can be executed.	please put emphasis on improvement of process insteadl of implementation of actual technical tools to ensure this being done.
4	University of Southern California Information Sciences Institute	Eileen Lu	E	12	471	482	3.1.1e	Is this to be a technical control or a procedural control? There aren't many systems out there that employ TPI in the sense of two people having to enter passwords for a command to run properly.	Please provide further clarification if procedural (two people signing off they performed the activity) is sufficient, or is it meant to be two people entering two different passwords?
5	University of Southern California Information Sciences Institute	Eileen Lu	E	12	483	490	3.1.2e	Question: how will this work if some one is part of the data supply chain where there will be upstream and downstream data sources/destination.	Please specify if user attestation and proper posture check re end point accessing restricted systems would suffice. Also, please help specific rules if one is part of the data supply chain and how that will work

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
6	University of Southern California Information Sciences Institute	Eileen Lu	E	13	514	515	3.1.3e	Cryptographic hash of file	this is not something can always be obtained. Please ;make sure to have emphasis on what's absolutely required consider if it can actually be implemented and what is not.
7	University of Southern California Information Sciences Institute	Eileen Lu	G	13	514	515	3.1.3e	The cost of hardware/software required to accommodate this logging requirement is not consider in the cost estimation.	please address this in the cost estimate report : https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf
8	University of Southern California Information Sciences Institute	Eileen Lu	E	16-17	N/A	N/A	3.4	The items in here seem to run counter to the "disinformation" suggestion from page 9. Overall it is giving a bit of a confusing approach to how things are supposed to be documented.	We would suggest for NIST to consider the "disinformation" concept needs to be downplayed if not eliminated. Or perhaps more clarifications/discussions are needed.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
9	University of Southern California Information Sciences Institute	Eileen Lu	E	16	573	586	3.4.2e	the cost of multiple software that will need to be employed not being considered into the Cost estimate in https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf This will also require efforts in developing the entire life cycle of the automation pipeline. The more complex piepeline is the harder it can work. Therefore some will be forced into creating multiple different automation pipelines that will require human resource effort to manage with continuous create, update and rollout.	Please consider keeping this flexible as it should just be recommended but not hard requirement as long as there is actual "process" but not automated would be a good starting point

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
10	University of Southern California Information Sciences Institute	Eileen Lu	E	25	772	785	3.11.3e	"the cost of multiple software that will need to be employed not being considered into the Cost estimate in https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf This will also require efforts in developing the entire life cycle of the automation pipeline. The more complex piepeline is the harder it can work. Therefore some will be forced into creating multiple different automation pipelines that will require human resource effort to manage with continuous create, update and rollout."	Please consider keeping this flexible as it should just be recommended but not hard requirement as long as there is actual "process" but not automated would be a good starting point

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
11	University of Southern California Information Sciences Institute	Eileen Lu	E	29	3.13.1e	877	906	the cost of multiple softwares, different use of security portocols, the human resource/personnels specialties all shoudl be considered into this control. the more diversity meaning the more personnel and tools to purchase - we don't feel it's being considered into the Cost estimate in https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-and-dod-cost-estimate-request-for-comments.pdf What is the baseline since the verbiage is creating so many possibilities.	please specify if this is just a soft guideline instead of being a hard standard
12	University of Southern California Information Sciences Institute	Eileen Lu	E	29-30	N/A	N/A	3.13.2.e	Simlar to the "disinformation", or this seems to be a practical application of it, We understand what is being promoted here. We think in reality though it is going to open the door for a lot of confusion on the end user/support side. Additionally it is likely people are going to introduce their own "tricks" to get around these changes. The end result is probably going to be less effective security not more.	We would suggest for NIST to consider the "disinformation" concept needs to be downplayed if not eliminated. Or perhaps more clarifications/discussions are needed.

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
13	University of Southern California Information Sciences Institute	Eileen Lu	E	29-30	N/A	N/A	3.13.2.e	It is also curious in this section that shortened credential time is mentioned, when earlier in the year didn't expiring passwords essentially become optional?	N/A
14	University of Southern California Information Sciences Institute	Eileen Lu	E	30	N/A	N/A	3.13.3e	Perhaps seemingly contrary to what has been written previously, this aspect of "disinformation" seems more "traditional", it is also being read though in the sense of being separated from the user base in general.	The last couple of criticism on this topic have mainly been in the sense of intermixing your "honeypot" and "live" networks is something that needs to be done very cautiously so as not to cause problems within the user community and potentially negatively impacting the overall security.
15	University of Southern California Information Sciences Institute	Eileen Lu	E	34	3.14.4e	1105	1105	we are concerned at least "twice annual" would be extremely difficult to achieve	please specify if this is just a soft guideline instead of being a hard standard

#	Organization Name	Submitted By	Type*	Page #^	Starting Line #^	Ending Line #	Section #	Comment (Include rationale for comment)^	Suggested Change^
16	University of Southern California Information Sciences Institute	Eileen Lu	E	9	4	4	Security Operations Center bullet	What is meant by "continuous monitoring"? Is this specifically eyes on a screen somewhere looking for issues, or automated tools and software that can send out alerts. An "operations center" would seem to imply the former, not every organization is potentially going to be able to support that. The latter is more workable.	Clarification footnote on whether this mean some of "manned" operation or use of automated tools and software. [Note after reading follow on paragraph, and later 3.6.1.e, perhaps just reference the section below about using external service providers.]
17	University of Southern California Information Sciences Institute	Eileen Lu	E	9	5	5	Disinformation bullet	I understand the concept being promoted here, the old "honeypot" machine but maybe to a greater extent. However, with how transitory employees are these days, espcially in the IT field, my concern would be these "disinformation" documents could become confused with real documents. This is potentially going to cause confusion and misconfiguration of machines and devices. Thereby decreasing security.	We would suggest NIST to consider that this concept needs to be promoted/approached with caution.