

August 2, 2019

The Honorable Walter G. Copan
Undersecretary of Commerce for Standards and Technology and NIST Director
National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

RE: Docket No.NIST-2019-0002: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets (June 19, 2019)

Dear Undersecretary Copan:

I write on behalf of the University of California, Los Angeles (UCLA) with regard to the special publication, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets”, published in the *Federal Register* by the National Institute of Standards and Technology (NIST) on June 19, 2019.

In fiscal year 2017, UCLA successfully competed for \$601.3 million in federal research funding. UCLA is committed to conducting research according to the University of California system-wide policy, which states that “[a]ll persons engaged in research at the University are responsible for adhering to the highest standards of intellectual honesty and integrity in research.”

According to the *Federal Register* notice, the aim of NIST’s proposed supplement to 171, 171B, is to articulate a set of enhanced security requirements around controlled unclassified information (CUI) in nonfederal systems and organizations for critical programs and high value assets. UCLA appreciates and strongly supports the need for appropriate and robust security and privacy across the research enterprise. However, we believe the requirements proposed in 171B may inflict unintended consequences on fundamental research and are cost prohibitive, burdensome, and unrealistic.

As written, the program change is unclear, particularly about when it would apply. In most cases, UCLA does not trigger SP 800-171 in accordance with the U.S. export control regulations and with Defense Federal Acquisition Regulation (DFAR) clause 252.204-7000, which states information arising out of fundamental research is not subject to disclosure controls. The NIST proposed change does not specify if fundamental research would fall under SP 800-171B. Unless agencies are mandated to state applicability in funding announcements, this proposed change

could be incredibly burdensome, as it is possible that applicants would not know that the award would fall under the new requirements until they are far along in the process of applying. Should awardees learn of requirements only at the time of contract, it may be impossible for them to comply, particularly within a timeframe that meets government contractual needs.

Even more fundamentally, it is important that NIST unambiguously state that the new requirements would not apply to basic research. In the absence of clear guidance, each agency could interpret differently what it considers “critical,” or an “advanced persistent threat,” or a “high value asset,” and may even require burdensome paperwork to prove compliance. Many areas that are of high value to U.S. adversaries represent a very wide range of technology and research including but not limited to AI, super computers, medical, specialized materials, biologics, genetics, agriculture, and computer science. While some agencies may view fundamental research in these areas as “critical” or “high value,” applying these security controls in such cases violates National Security Decision Directive 189. The NIST guidance should make clear these controls are inappropriate for fundamental research.

The proposed change is potentially cost prohibitive for universities, reaching into the tens of millions of dollars. 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 would be excessive and unaffordable. This could prevent institutions seeking to conduct important research for the government from doing so.

Managing both sets of security requirements for CUI (800-171 and 800-171B) is unduly burdensome. Essentially it requires building a 171 environment and adding the 171B requirements on top. There is potential for confusion, both on the part of federal agencies and universities, as to which set of requirements would apply in a given instance. While the guidance refers to equally effective alternative measures, it would be useful for NIST to provide specific examples and guidance on how that equivalent effectiveness may be determined.

The proposed change doesn't seem to take into account the level of complexity, sophistication, and cost required to deploy some of the controls (i.e., disrupting the attack surface through unpredictability, moving target defense, or non-persistence). Expecting universities to implement these controls on any kind of immediate basis is completely unrealistic. At the least, the guidance should allow for multi-year or phased-in adoption of the controls.

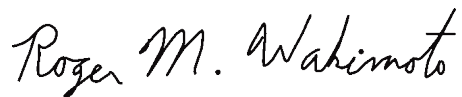
Some of the security controls involve costly tactics and counterintelligence activity as opposed to defensive security measures, such as penetration testing by designated agents and red teams; deception to confuse and mislead adversaries; no-notice social engineering attempts against individuals to gain unauthorized access; the conduct of enhanced personnel screening (vetting) for individual trustworthiness (even when the CUI level doesn't warrant enhanced vetting); and misleading adversaries through a combination of misdirection, tainting, or disinformation. It is unclear what the ramifications may be of some of these endeavors, particularly in a university context where the culture necessitates openness and sharing.

The requirement (3.6.1e) for a full-time, 24 hours per day, seven days per week, personnel-staffed security operations center creates prohibitive operational cost, especially with regard to

federally-funded university research. The objective of such ongoing monitoring, including detection, alerting, and response, can be accomplished through the use of automated tools. Organizations should be allowed to tailor their approach to meet the objective of ongoing monitoring using their own best-fit combination of technology and personnel rather than a specific requirement for staffing. Note that this change would also be consistent with industry trends leaning toward automation and technology tools in place of additional human resource investment.

In conclusion, the proposed new requirement is inconsistent with current policies and would impose significant cost and administrative burdens on universities, likely prohibiting them from conducting important research for the federal government. UCLA urges NIST to reconsider the implementation of (SP) 800-171B.

Sincerely,

A handwritten signature in black ink that reads "Roger M. Wakimoto". The signature is written in a cursive, flowing style.

Roger Wakimoto, Vice Chancellor of Research and Creative Activities