August 19, 2020

National Institute of Standards and Technology
United States Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

Re: Draft NIST Special Publication (SP) 800-172, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations – Enhanced Security Requirements for Critical Programs and High Value Assets.

To Whom It May Concern:

As an association, NDIA represents more than 1,600 corporate and over 80,000 individual members from small, medium, and large contractors; our members and their employees feel the impact of any policy change made in how the United States equips and supports its warfighters. Our comments provided below come from this diverse membership and represent a broad range of perspectives across the defense industrial base (DIB).

NDIA and its members welcome the opportunity to comment on the recently issued updated draft NIST SP 800-172 and are truly appreciative of all the efforts NIST has dedicated in developing standards to govern contractor networks with controlled unclassified information (CUI). As you know, the defense industrial base has long urged the Government to avoid a patchwork of disparate cybersecurity requirements applicable to the federal supply chain, and instead advocated for the adoption a single framework of cybersecurity controls to facilitate the ability of DIB companies of all sizes to implement compliant systems and networks. Today, outside of DoD, most civilian agencies and their components have yet to require compliance with NIST SP 800-171, and DoD is preparing to shift from NIST SP 800-171 to the Cybersecurity Maturity Model Certification, which consists of five (5) maturity levels, issued earlier this year. At the same time, many contractors are still working to conform to each of the 110 NIST SP 800-171 controls.

Given the evolving threats, we understand that there is a need to require additional controls when the nature of the risks associated with the program or technology are heightened and thus support the issuance of NIST SP 800-172. NIST, in developing controls to address enhanced risks, however, now seeks to recommend NIST SP 800-172 enhanced requirements that deviate from the CMMC Level 4 and Level 5 processes designed to address the same elevated risks. In fact, it appears that less than half (only 15 of the 34) of the recommended NIST controls directly align with the CMMC processes finalized in January 2020. Notably, the CMMC processes were developed in close collaboration with industry experts with a focus on identifying implementable requirements that would provide the needed additional protections while avoiding excessively expensive requirements that did not provide much security value and that many

contractors, particularly small and medium businesses, may not be in a position to implement. We recommend that NIST, in finalizing its controls, prioritize enhanced requirements that better align with the CMMC processes to the maximum extent possible to facilitate contractor compliance. Such alignment will encourage agencies or individual programs to discontinue the unfortunate and arguably counterproductive practice of developing their own unique cybersecurity requirements that exceed both the draft NIST SP 800-172 and CMMC requirements. Compliance with the proliferation of requirements is not cost effective for contractors or the Government and can create risks for companies that lack the resources to track emerging and evolving developments in real time or implement redundant individualized controls. Indeed, one of the primary purposes of the CUI rule was to implement Executive Order 13556 (CUI EO), which had a goal of addressing the ad hoc, agency-specific approach to safeguarding and managing such information. The current approach may frustrate work over a decade in the making.

With respect to the fifteen (15) NIST SP 800-172 enhanced requirements that align to CMMC Level 4 and 5 processes, NDIA noted that NIST has altered the specific language of the CMMC processes, which may lead to unnecessary confusion and ambiguity as to what constitutes compliance with these specific requirements. Thus, NDIA recommends that NIST consider using the same language as in the CMMC processes whenever possible when finalizing the NIST SP 800-172 enhanced control requirements.

NIST advises federal agencies in its draft that the NIST SP 800-172 controls should be considered for use only when associated with "critical programs" or "high value assets," which are the potential targets of an advanced persistent threat (APT), and further clarifies that the enhanced security requirements only apply to components of non-federal systems that include or protect CUI associated with a critical program or high value asset. Notably, NIST recognizes in footnote 6 that the definition of "critical program" varies from agency to agency. Given this variation, NDIA recommends that NIST provide more guidance as to what constitutes the type of critical programs and high value assets likely to be a target of an APT. Absent such clarification, there is risk that federal program managers would apply these controls in an overly broad and/or inconsistent manner, unnecessarily utilizing agency and contractor limited resources.

Crucially, NIST does not call for wholesale adoption of all 34 of the recommended NIST SP 800-172 controls on these select programs but rather calls for flexible application of the controls. We applaud NIST's clear statement "that there is no expectation that all of the enhanced security requirements will be selected by every federal agency" for each critical program or high value asset. We support the concept that elevated requirements should be carefully selected and tailored to specific programs' needs to ensure that costs and resources are not wasted, although we reiterate our statements above that the requirements should align with CMMC to the maximum possible extent. We are concerned that not all agencies will be well positioned to assess the risks and select the set of enhanced requirements based on the mission protection needs associated with a particular program or asset. Agencies may decide to take a risk averse approach by imposing greater requirements than needed (i.e., an "all of the above" approach or a confusing combination of options from different standards). NDIA recommends that additional guidance, consultation and training be available to federal employees involved in such decision-making. It is important that the rules applicable to industry are repeatable, consistent, and predictable regarding both an initial cost and a sustainment perspective.

In addition to assessing the risks and selecting the appropriate controls to apply, NIST appears to empower the federal agencies, not the contractor, to tailor the "to be defined" parameters embedded in many of the

individual controls by identifying specific values. (See "Quick Tips for Federal Agencies" on page 10, and footnote 17). This principle contradicts the approach taken for NIST SP 800-171 and the NIST Cybersecurity Framework, which was designed to provide flexibility for contractors in how to implement controls given that contractor systems vary and that there is no exclusively correct way to accomplish the controls. We are concerned that if various agencies are given discretion to set specific, varying parameters on various controls, the result would be a mishmash of inconsistent yet very burdensome requirements being levied on contractors by various agencies in an uncoordinated and ad-hoc fashion. In addition, it is unclear whether each agency has the required resources or insight necessary to make security determinations on behalf of contractors and the result of having individual values assigned by agencies will likely lead to varying application by agencies upon contractors and lack of predictability for the contracting community. As a result, we note the very real possibility that contractors will be forced to implement the requirements using varying, agency-mandated parameters within their infrastructure and potentially even on the same systems, which adds unnecessary costs, wastes valuable resources and creates unnecessary compliance complications (e.g., multiple audits of the same system using differing standards). In this light, we note that many CMMC controls allow system owners to be defined parameters based on a risk-informed analysis, in a nod to the fact that system owners themselves are best acquainted with the risks facing their information systems. We recommend that the NIST SP 800-172 controls reflect the same underlying principle.

The NIST SP 800-172 document calls for physical and logical separation of environments and controlled information flows across those environments (3.1.3e & 3.13.4e), and the cost for compliance is perceived to be very expensive to achieve an air-gapped and completely segmented network separated from any other internal environment that allows only physical transfer of data (e.g., information, updates, patches). Although the costs for the segregated network may be built into certain contract types, the initial startup costs will be high and may be unrealistic for certain size contractors and subcontractors to achieve. Access to shared enterprise applications such as email, collaboration, and storage become untenable in a fully implemented segregation environment (like a classified system), which means that contractors would have to implement separate and independent business applications into the segregated environments. Doing that for a SharePoint system or file server may not be unduly expensive, but having to replicate eMail and collaboration systems into every enclave is counter to the recognized concept of sharing resources to achieve efficiency and reduce costs to the USG customer. This model becomes even more problematic as companies migrate their internal systems to the cloud. While the need is understood and implemented in classified environments, NIST should add further clarification as to when these controls should apply and why they are necessary given the immense difficulty and cost burdens they bring to CUI environments.

Finally, NIST, in its draft, acknowledges that certain of the enhanced security requirements may be too difficult or cost prohibitive for contractors to implement internally and recommends leveraging external service providers. While this certainly may at times be a viable alternative to some companies, this may not be feasible or cost effective depending on the number of internal systems or scope of infrastructure subject to such requirements especially since different systems may be subject to different requirements depending on the requirements imposed on the programs they support. If there are to be segregated environments, then use of external service providers also may not be practical because they tend to be "shared" services outside of the contractor and would require "reach in" access to the program. This would increase the customer's security risk, not reduce it, even "if" the cost of the external service provider is less than what it would take for the contractor to do it themselves. External service providers also would be prime targets for adversary attacks and would likely need to obtain their own CMMC and similar certifications for each environment they are managing. That may not be economically practical.

Thank you for your continued efforts to solicit industry feedback on draft and proposed documents, like SP 800-172. If you or your staff have any questions, please contract Corbin Evans, Principal Director of Strategic Programs, at cevans@ndia.org or (703) 247-2598.

Respectfully Submitted,

National Defense Industrial Association