2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

June 11, 2021

Charles H. Romine, Director, Information Technology Laboratory
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930)
Gaithersburg, Maryland 20899-8930

Re: Draft NIST Special Publication (SP) 800-172A Assessing Enhanced Security Requirements for Controlled Unclassified Information

Mr. Romine:

The National Defense Industrial Association (NDIA) represents more than 1,600 corporate members 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).

I. General Comments and Recommendations

NDIA and its members welcome the opportunity to comment on the recently issued updated draft NIST SP 800-172A and are truly appreciative of all the efforts that the National Institute of Standards and Technology (NIST) has dedicated in developing standards to govern contractor networks with controlled unclassified information (CUI). 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 companies of all sizes to implement compliant systems and networks. Today, outside of the Department of Defense (DoD), most civilian agencies and their components have yet to require compliance with NIST SP 800-171 as DoD is preparing to shift from NIST SP 800-171 to the Cybersecurity Maturity Model Certification (CMMC), which consists of five 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.

NIST, in developing assessment standards for controls aimed at addressing enhanced risks, however, continues to deviate from the CMMC Level 4 and Level 5 Practices designed to address the same elevated risks. In fact, it appears that less than half (only 15 of 35) of the recommended NIST controls directly align with the CMMC processes finalized in January 2020, in CMMC v1.02. 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 consequential security value and that many contractors, particularly small and medium sized businesses, continue to not be in a position to implement. We recommend that NIST, in finalizing its controls and the associated assessment standards,

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 NIST SP 800-172 and the 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 Executive Order 13556 (CUI EO) and the recent Executive Order on Improving the Nation's Cybersecurity, is the 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 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. This process of reconciliation should also be conducted for 172A and the forthcoming assessment guide for CMMC Level 4 and 5.

Crucially, NIST does not call for wholesale adoption of all 35 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 from both an initial cost and 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 Practices 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 and assessment guide reflect the same underlying principle.

II. Comments on Preface Materials

Included in the Abstract is the statement "The assessment procedures are flexible and can be tailored to the needs of organizations and assessors." NDIA is concerned by reports of early assessments by the Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center assessments of companies using the NIST SP 800-171A that the spirit of this statement is being lost and a rigid, inflexible methodology is being employed by assessors. We recommend that this statement and sentiment be elevated and present throughout the document to further accentuate the need for a flexible approach to assessments.

It has been broadly discussed that compliance with any current federal standard is not in itself a failsafe security solution but instead a foundation and starting point, therefore we recommend that lines 94-98 are reprinted in the final draft of the assessment guide, not just included for reviewers of this draft.

There are several statements presented in the preface material of this publication that if accepted in the final would have the effect of NIST expanding the scope and jurisdiction of the coverage of this document. Two statements that would result in an expanded scope of this regulation and require additional systems to be covered by the enhanced requirements of NIST SP 800-172 are 1) "The enhanced requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high value asset[,]" and 2) "[t]he requirements also apply to services, including externally provided services, that process, store, or transmit CUI, or that provide security protections, for the system requiring enhanced protection." Another statement that again expands the scope beyond what was included in the Federal Register, resulting in more companies, systems, and procedures being swept up to the enhanced security requirements is "Federal agencies may limit application as long as the needed protection is achieved, such as by applying the enhanced security requirements to the components of nonfederal systems that process, store, or transmit CUI associated with a critical program or high value

asset; provide protection for such components; or provide a direct attack path to such components (e.g., due to established trust relationships between system components)." This statement again expands the scope beyond what was included in the Federal Register, resulting in more companies, systems, and procedures being swept up to the enhanced security requirements. As we have seen with NIST SP 800-171, ambiguity leads to rigid and inflexible interpretations of the regulations and imposes undue costs and complexity on an already arduous system of security compliance. We recommend that NIST reconsider these statements and clearly state in the final publication what is intended to be included in the assessments associated with this publication.

Line 52-54. The Abstract states that "[t]he protection of unclassified federal information in nonfederal systems and organizations is dependent on the Federal Government providing a process for identifying the different types of information that are used by federal agencies." This statement is an excellent point for why the Federal Government's proper marking of CUI is foundational to this entire program.

Lines 58-64. A "flexible" and risk-based decision-making approach is not being currently applied by the Defense Contract Management Agency (DCMA) in all instances.

III. Comments on Reviewers section

There is no expectation that all assessment methods and assessment objects will be selected for each assessment procedure. Rather, the procedures should be used by organizations as a starting point for developing *a System Security Plan* and approaches that can produce the evidence needed for risk-based decisions or to determine compliance to the CUI enhanced security requirements.

We need to ensure that third-party assessors do not require every potential assessment method and object for each enhanced control. Each company will be different in applying the Controls and they may not match exactly but will still be capable of making risk-based decisions and protect the data. This will once again become a check-the-box mentality and will not allow for flexibility on the part of the assessed organization.

Line 84. How are "flexible and tailorable assessment procedures for the CUI enhanced security requirements" explicitly being made flexible and tailorable.

Line 90. How is the statement "Facilitating different levels of assurance in security assessments by varying the scope and rigor of the assessment through selectable depth and coverage attributes;" being applied. The remainder of the assessment guide does not seem to address this.

Line 94-98. These lines should be included in the final not just draft for reviewers.

IV. Comments on the Procedures

Line 374. The word “organization” is used twice in the same sentence and may not mean the same organization. In the first case they mean the Assessing Organization. In the second case, it may mean the organization that has called for or required the enhanced security requirements (e.g., the Government).

Line 392. Please clarify the use of the word “organizations.” Is it the Government, the Assessor, or the OSC?

3.1.1e. This Control does not mention Automation yet in the Test section of Assessment methods and objects it uses the word “Automated.” An assessor will invariably ask to see how an organization being assessed is automating the process. Remove the word “Automated” and replace with “Review.” Employ dual authorization to execute critical or sensitive system and organizational operations.

3.1.1e. The word “Automated” is in the Test section of almost every Control which in many cases is not practical or possible.

3.1.2e. The requirement outlined by this procedure is potentially impossible to meet in a Cloud environment. By their nature, Cloud will have some components that are not owned, provisioned, or issued by the organization. It also has the impact of eliminating the ability to use Managed Service Providers (MSPs), which are recommended by NIST itself earlier in the document as one alternative to mitigate the cost of implementation. Clearly the intent of this control is to eliminate “bring your own devices policies” but considering a scenario where the Federal government or the CMMC program applies this enhanced requirement, it effectively ends both MSP and CSP use, and forces an on-premises-only architecture for the organization seeking certification (OSC). We recommend that the assessment objectives for this control should be modified to exclude Cloud and MSPs (which have other requirements like FedRAMP, etc.).

3.2.1e[a]. “Threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors are identified.” We recommend that this requirement be dropped from the final assessment guide. The word “identified” in assessment terminology means a specific listing of threats and their tactics, techniques, and procedures (TTP) must be developed and maintained by the OSC. In general, threats are frequently changing, are identified in a myriad of ways, and organizations like the Defense Cyber Crime Center (DC3) maintain up to date lists of these advanced persistent threat TTP’s. Any “identified” list would likely be out of date shortly after it was written, creating a difficult requirement for the OSC to successfully fulfill, and resulting in negligible security improvements. Assessment objective [b] is sufficient for this control to be effective in achieving its goal.

3.2.1e[a]. The complexity and lack of return outlined above holds true for procedure 3.2.1e[c], and we similarly recommend that this procedure be dropped. 3.2.1e[d] should instead be modified to include “are

identified" at the end of that AO. NDIA recommends that NIST avoid driving the expansion of the requirement to now requiring the maintenance of lists that are freely available and add no value while driving administrative cost and complexity into the system.

3.2. We recommend that procedures 3.2.2e[a] and 3.2.2e[b] be dropped for a similar reason we recommended above with procedure 3.2.1e[a]. Again, this requirement is asking the OSC to create and maintain lists to be examined that do not enhance security. Procedures 3.2.2e[c]-[e] are sufficient to achieving the goal of this control.

ODP 3.4.2e[1]. "One or more of the following is/are selected: remove the components; place the components in a quarantine or remediation network." It is unclear whether unauthorized systems components are authorized for connection to the system at all under the current 3.1.1[f] security requirement/assessment objective. If the control outlined in 3.1.1[f] is being met, then the unauthorized part of this is already covered. We recommend modifying this section by adding a selection to this ODP for never letting an unauthorized or misconfigured component to connect to the system in the first place. If 3.1.1 is fully implemented and the organization is in compliance with NIST SP 800-171, this scenario never develops. This requirement is not a moderate maturity activity. It is a high-level maturity activity currently being required for basic and moderate systems because of the way NIST SP 800-171A was written.

ODP 3.4.2e[1]. Also, for consistency, subsections [a] should be swapped with subsection [c] in the list, and sections [b] and [c] should be moved up.

3.4.3e. We recommend that assessment objective [b] "Up-to-date, complete, accurate, and readily available inventory of system components exists" be dropped. The requirement of this procedure sets an assessment bar for having a perfect inventory and means any single inventory discrepancy can result in a failure for an entire assessment. The government is currently incapable of doing this on their own networks and should not try to hold the DIB accountable to this standard. DIB companies vary in size and complexity and the requirement associated with this procedure could result in the compilation and maintenance of inventories of tens-of-thousands of connected system components.

3.5.1e. "Identify and authenticate [Assignment: organization-defined systems and system components] before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant." This procedure seems to reference device authentication, which is not generally a standard practice in current IT implementations. Instead, current systems focus on the authentication of individuals accessing a system. The procedure here should instead by focused on the requirement to authenticate individuals and passwords, not ensuring that every laptop on a system also contains a password. NIST 800-63-3, the reference for procedure specifically puts device authentication currently out of scope and speaks to instead focus on authenticating identity. While the ODP seems to clarify this, assessment objective [c] again creates confusion. After reviewing the reference (800-63-3) what the control appears to be requesting is not supported in the reference, stating "The requirements detail the acceptability, validation, and verification of identity evidence that will be presented by a

subscriber to support their claim of identity," which is not inherently related to individual devices. It seems difficult, and potentially impossible to fashion a network device authentication requirement in the fashion this control seems to call for.

3.5.1e. A related problem is present in procedure 3.13.11: "Employ FIPS-validated cryptography when used to protect the confidentiality of CUI." By calling for cryptographic mechanisms that "provide security" for CUI systems, NIST is expanding the scope well beyond what is included in the DFAR rule defining covered system. If maintained, this procedure would require the organization to invoke the need for this cryptographic mechanism to be FIPS Validated. Where the standards reference "cryptography," we interpret that it invokes the requirement that it then "must always be FIPS validated." This procedure as written, if enforced has the potential to eliminate all commercially available identity solutions. Outside of the FIPS Validated requirement, most commercially available solutions today already comply with the standards of this procedure (for people but not devices).

3.11.4e. "Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination." Although executable in keeping with the assessment objectives, we recommend that an example of what a real-world application looks like from NIST's perspective. This procedure, as written, is not sufficiently specific to provide adequate guidance to an organization seeking certification.

Thank you for your continued efforts to solicit industry feedback on draft and proposed documents, like SP 800-172A. 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 or Nick Jones, Director of Regulatory Policy, at njones@ndia.org.

Respectfully submitted,

National Defense Industrial Association