[redacted]

From: "Timm, Jason" [redacted]
Date: Monday, September 19, 2022 at 4:18 PM
To: sec-cert <sec-cert@nist.gov>
Subject: AIA Comments to NIST SP 800-171 Pre-Draft Rev 3

Dear NIST,

Apologies for the late response as we were unable to submit the attached on Friday evening, 16 Sep.

I hope you are willing to accept our attached comments and that you find them useful as you continue your work on Rev 3.

V/R

Jason

Jason Timm | *Director, Defense Policy & Integration*
AIA | 1000 Wilson Boulevard, Suite 1700, Arlington, VA 22209
[redacted]
aia-aerospace.org

AIA
AEROSPACE
INDUSTRIES
ASSOCIATION

September 16, 2022

National Institute of Standards and Technology
Computer Security Division
Computer Security Resource Center
Email to: sec-cert@nist.gov

RE: NIST Special Publication (SP) 800-171 Rev. 3 Pre-Draft Call for Comments: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

Dear NIST:

On behalf of the Aerospace Industries Association of America (AIA), I am pleased to offer the enclosed comments in response to NIST Special Publication (SP) 800-171 Rev. 3 Pre-Draft Call for Comments: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

For over 100 years, AIA has been the industry voice shaping policies that matter most to our nearly 330 members, which includes the nation's leading aerospace and defense manufacturers and suppliers of civil, military, and business aircraft and engines, helicopters, unmanned aerial systems, space systems, missiles, equipment, services, information technology, and other related components.

AIA believes that lessons learned demonstrate how requirements and processes in cybersecurity are mutually beneficial when shared through robust collaboration across sector business operations representing all stakeholders. AIA is committed to initiatives that secure information from cyber threats and we continually work to encourage collaboration between industry and government on cybersecurity matters to include innovation, agility, and flexibility across all businesses and government entities supporting national and international missions.

Thank you for the opportunity to provide these comments and concerns.

Sincerely,

Jason Timm
Director, Defense Policy & Integration, National Security Policy

Enclosure: AIA Comments to NIST Pre-Draft Call for Comments to NIST SP 800-171 Rev 3

AIA Comments to NIST Pre-Draft Call for Comments to NIST SP 800-171 Rev 3

General Comments:

Establishing an adjudication process for public comments

Minimal changes were made between the NIST SP 800-171 Rev 1 and Rev 2 releases, and it seems that most public comments provided have not been reflected in Rev 2. AIA is concerned that this may result in NIST potentially setting a precedent discouraging nonfederal industry entities from applying resources and subject matter expertise to support publication reviews and comment submissions, thereby challenging NIST's mission to benefit industry and U.S. industrial global competitiveness. Additionally, CUI publication standards are already cited by current and planned regulations across nonfederal entities, and it is operationally vital to have an adjudication process for tracking changes to CUI Publications that are impacted by new and updated laws and regulations, such as:

- DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting,
- DFARS Case 2019-D041, Strategic Assessment and Cybersecurity Certification Requirements, which introduces the Cybersecurity Maturity Model Certification (CMMC) into DFARS language, and
- NARA FAR Case 2017-016, Controlled Unclassified Information (CUI), which includes future expansion across government to critical infrastructure.

AIA encourages NIST to adopt a formal adjudication process for public comments to maximize participation and reduce the potential for deviations across current and planned domestic and international cybersecurity frameworks and standards.

Establish reference documents for control selections (including enhanced controls)

AIA notes that previous drafts of NIST SP 800-171 Rev 2 were not updated to adequately identify when enhanced controls would apply to programs or assets and states, "*The enhanced security requirements are applied, as necessary, to protect CUI associated with a critical program or a high value asset.*" While NIST updated the definitions for "high value asset" and "critical program (or technology)", these changes failed to provide reference documents, conditions, or guidance for how a risk determination is made by a private entity for nonfederal acquisitions that could constitute as a "critical program". In addition, the updated statements in the NIST SP 800-172 for "maximum flexibility" and control selection, and subsequent steps provided by the "*Implementation Tips for Federal Agencies*" do not clearly define an established process for selecting enhanced controls and control assignments. The lack of clarity in this area not only impacts the ability of the defense industrial base (DIB) (and potentially other organizations) to provide effective comments on controls, and assess the full financial impacts proposed by enhanced controls on contractors, but could also lead to:

- inconsistent and arbitrary selection of enhanced controls and control assignments
- inconsistent application by agencies
- a lack of predictability for the contracting community

- increased costs for programs that may not be critical
- less than desirable effectiveness of the CUI publications

AIA recommends that NIST provide reference documents for guiding control selections so that inconsistencies between agencies can be resolved.

Provide minimum acceptable values for Organizationally Defined Requirements (ODRs)
The lack of minimum acceptable values for controls containing ODRs will likely lead to an uneven application of the standard across the DIB. The lack of standard "best practice minimums" for ODRs will require companies, assessors, and government sponsoring agencies to individually interpret the implementation intent of the specific controls. Companies may make a risk-based analysis, incorporating ROI, staffing, or high-risk tolerance, that renders the control ineffective. However, that risk assessment nonetheless defines their "organizationally defined requirement". Assessors may refer to their individual experience, training, and temperament to determine whether a documented ODR is "good enough". Finally, sponsoring agencies will likely be inclined to provide their own standard best practice guidance, which may be conflicting across agencies, resulting in an additional coordination burden for companies supporting multiple government sponsors.

To ensure consistency, AIA recommends that NIST propose minimum acceptable ODR values that match its implementation intent for the NIST SP 800-171. Coordinating those proposed values with a sampling of DIB companies across the supply chain and posting the results of that coordination in future 800-171 revisions would provide the DIB guidance on a projected range of values.

FIPS encryption and Multi-Factor Authentication (MFA) control sets
Controls regarding FIPS implementation and MFA present challenges for DIB implementation due to issues around converting government-specific requirements to non-federal systems and selecting the best implementation options from the variety of commercial solutions available (especially for FIPS implementation). FIPS and MFA guidance do not provide enough specifics on how to acceptably use commercial solutions which provide features and options that allow for flexible implementation. For example, the DCMA DIBCAC presented the following data at the on September 13: of the 117 DIBCAC High Assessments they performed over the last 3 years, 51% of companies were Other Than Satisfied (OTS) (Not Met) for the FIPS requirement due to the lack of options or misconfigurations. Additionally, 38% were OTS for MFA primarily due to the lack of options on many devices combined with lack of network segmentation. These numbers do not show the percentage (as described by DCMA DIBCAC) that had these identified as satisfied via POA&Ms for enduring exceptions or temporary deficiencies (awaiting the FIPS validation of new versions) which was attributed to a large portion of the organizations that passed. Since not all FIPS products operate in the same way, and a customer organization has no way of knowing whether that product's implementation (not algorithm), is acceptable, this could result in confusion between companies and assessors about whether the implementation of a specific product meets the intent of the 800-171.

As a result, AIA recommends that NIST provide additional guidance and/or reassess the requirements/controls such that they are meaningful, measurable, and attainable while also secure and meet the intent of the requirements/controls. AIA stands ready to work with NIST to create publications which clarify FIPS and MFA requirements for private industry and provide guidance to 800-171 users on proper FIPS-certified product implementation.

Flexible implementation of NIST SP 800-171 controls to accommodate all types of technologies
For some federal agencies, implementation of the 800-171 means application of all 110 controls is mandatory, but not always feasible because some controls may be deallocated with a sufficient business justification. Additionally, to address their individual risks, there is a need for flexibility and risk assessment in determining what is needed for adequate security for different contractors, in different sectors, falling under different tiers in the DIB. For example, systems using non-traditional login methods may not require certain identity and access management controls because having them could adversely impact mission operations. In addition, a flat, check-the-box standard does not meaningfully address the emerging types of threats that the DIB must protect against.

AIA Recommends having a control tailoring process or level of effort (LOE) decision tree for performing a cost-benefit analysis and determining the applicability of controls and requirements within a private industry organization. In addition, having a process that identifies which controls are “most important” will help with the control selection process and determining alternative solutions for controls that have been deallocated.

Establish a single framework with one set of controls, or provide clearer guidance on how and when to apply the various frameworks
The use of multiple frameworks, each with unique security requirements, has led to:

- Unclear or conflicting guidance received from different Executive-branch Agencies, making it difficult to determine and appropriately plan for implementation of security requirements.
- Requirements changing based on personal interpretations of how to apply or assess security controls, causing confusion about what may or may not apply in each circumstance.
- Conflicts between related publications that are not on the same scheduled for reviews and updates.
- Difficulty in determining equivalency between frameworks because of the different control requirements, especially when dealing with frameworks that are not maintained by NIST (i.e., CMMC, FedRAMP, UK Cyber Essentials, etc.)

AIA recommends having a single Risk Management Framework (RMF) with one set of security controls that includes the baseline requirements for all current scenarios (CUI on non-federal systems, FedRAMP, federal information systems, etc.). If a single framework is not possible, then AIA recommends that control mappings be expanded to include frameworks outside of NIST, creating appendices that better explain the relationship between frameworks, updating control information to include references to associated frameworks and controls, and providing clearer guidance on when and how to apply the various frameworks.

Updating the information types listed in the NIST SP 800-60 to include CUI categories

The information types listed in 800-60 do not address or include the categories of CUI listed in the CUI Registry. Meanwhile, overarching guidance for CUI only considers confidentiality for protection, and excludes other important triad areas of protection that will help diminish the risk surface creating a gap in the process for appropriately selecting security controls. This can make it difficult to determine:

- The relationship between CUI categories and control requirements as it does not account for additional or differing control requirements for CUI Specified.
- Application of controls in environments where the “high-water mark” (i.e., the baseline set of requirements depends on the security objective (confidentiality, integrity, and availability) with the highest value assigned) approach may not be used.
- The resources that can be shared between multiple programs where supported agencies follow different authorities or have their own unique control requirements.

While AIA does not recommend defining more categories of CUI, we do recommend NIST update the 800-60 to include the CUI categories and types (basic and specified) and provide overlays that cover the different requirements for CUI Specified as this can help to close these process gaps. Additionally, AIA recommends NIST develop a well-defined process for identifying CUI which would also be helpful in simplifying the review and approval of potential CUI.