

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

7 Jun 2018

Ms. Mary Thomas
OUSD(A&S) DPAP/PDI, Room 3C958
3060 Defense Pentagon
Washington, DC 20301-3060

Ref: DARS 2018-0023

Dear Ms. Thomas:

The Council of Defense and Space Industry Associations (CODSIA)¹ is pleased to offer our comments in response to the Department of Defense (DoD) Request for Comment on the DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented (Docket DARS–2018–0023).

In an effort to better collaborate with DoD to enhance the security of defense information throughout the aerospace and defense industries, two documents are attached containing general and specific comments found in an ‘in-line’ format.

In addition, below are some overarching comments:

- Clarification is required to ensure that the unimplemented controls information and SSP/POAM are for the prime contractors only. Due to the lack of contract privity and visibility to lower supply chain levels, obtaining and managing this information at all levels of the supply chain would be unmanageable.
- The stated purpose of the ‘Not Yet Implemented’ document is to facilitate the consistent review and understanding of System Security Plans and Plans of Actions to assist in the prioritization of unimplemented controls; however, NIST values 93 of the 110 controls (85%) as Priority 1 and DoD values 91 of the 110 (83%) controls as highest priority. This minor difference does little to assist contractors in setting implementation priorities.
- DOD continually stresses the need for innovation and faster delivery of advanced capabilities to the warfighter. In our view, focus of the NIST SP 800-171 Security





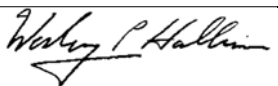


¹ CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of seven associations – Aerospace Industries Association (AIA), American Council of Engineering Companies (ACEC), Associated General Contractors (AGC), Information Technology Alliance for Public Sector (ITAPS), National Defense Industrial Association (NDIA), Professional Services Council (PSC), and U.S. Chamber of Commerce. CODSIA’s member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members’ positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

Requirements on the specific details of industry compliance adds complexity and time to the acquisition process. Every effort should be made to streamline the approach and adapt to a threat-based, rather than compliance-based, approach to cybersecurity.

Thank you for your attention to these comments. If you have any questions or need any additional information, please contact Jason Timm of the Aerospace Industries Association, who serves as our project officer for this case. He can be reached at jason.timm@aia-aerospace.org or (703) 358-1043.

Sincerely,

	
John Luddy Vice President National Security Aerospace Industries Association	Steve Hall Vice President, Government Affairs American Council of Engineering Companies
	
Jimmy Christianson Regulatory Counsel Associated General Contractors of America	A.R. "Trey" Hodgkins, III, CAE Senior Vice President, Public Sector Information Technology Alliance for the Public Sector
	
Wesley P. Hallman Senior Vice President for Policy National Defense Industrial Association	Alan Chvotkin Executive Vice President and Counsel Professional Services Council
	
Neil L. Bradley Senior Vice President & Chief Policy Officer U.S. Chamber of Commerce	

2 Enclosures:

Encl 1 Comments to DoD Guidance for NIST SP 800-171 Requirements Not Yet Implemented

Encl 2 Comments to Matrix for Assessing Contractor's Internal System in Procurement Action

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

Enclosure 1

**DOD GUIDANCE FOR REVIEWING SYSTEM SECURITY PLANS AND THE NIST SP
800-171 SECURITY REQUIREMENTS NOT YET IMPLEMENTED**

GENERAL INDUSTRY COMMENTS:

1. The stated purpose of the 'Not Yet Implemented' document is to facilitate the consistent review and understanding of System Security Plans and Plans of Actions to assist in the prioritization of unimplemented controls; however, NIST values 93 of the 110 controls (85%) as Priority 1 and DoD values 91 of the 110 (83%) controls as highest priority. This minor difference does little to assist contractors in setting implementation priorities.
2. There needs to be an internal process within DoD to vet program specifics above and beyond the NIST SP 800-171 security requirements.
3. Adequate Security for specific types of CDI is not yet defined. Without properly defined CDI, how will programs know what is considered adequate security or acceptable risk especially considering not all controls may be implemented?
4. Providing a more specific/narrow definition of CDI as part of the procurement process will allow contractors to better identify, isolate, and protect CDI.
 - a. How will CDI be identified? Although identifying and marking CDI is the responsibility of the DoD, one challenge contractors have encountered is that CDI is rarely identified or marked, and thus contractors have no way to know what is or is not CDI.
 - b. In the event CDI is not clearly identified or marked, what is the course of action contractors should take to ensure they have a clear understanding of what constitutes CDI under a contract?
5. The information necessary for the Government to make an independent assessment is highly sensitive both for security and competitive reasons. How will the Government assure contractors their information will be kept secure? How will this information be transmitted to, stored by, controlled by and destroyed by the Government?
6. Clarification is required to ensure that the unimplemented controls information and SSP/POAM are for the prime contractors only. Due to the lack of contract privity and visibility to lower supply chain levels, obtaining and managing this information at all levels of the supply chain would be unmanageable.
7. How will the Government manage/monitor implementation of POAMs?
8. Are POAMs that are incorporated into a contract a fixed set or would they be updated during the contract lifetime?
9. Security Assurance Levels (which provide a qualitative approach to addressing security for a specific zone or control) can be used to establish the need for additional support due to criticality of the data in procurements.
 - a. Information on SALs:

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=906330

SPECIFIC INDUSTRY COMMENTS BY CONTROL

3.1.4

- Guidance is required regarding small organizations with 1, or very few IT staff, as separation of duties may not be possible or operationally practical.

3.1.6

- Example scenarios should be added for assessment clarity such as 'firewall administrators should use a non-privileged account to read email and a privileged account to administer the firewall.'
- DOD could add 'for applicability in assessment' to the terms related to security and system administrators. This may provide clarification in permitting local user administration functions to be granted such as for users to install software.
- Clarify that this requirement is only related to users who have local administrative privileges on endpoints to install software.

3.1.7

- Recommend assessment clarity to separate administrative users' roles from editing audit logs.

3.1.9

- Recommend DOD provide a sample or template of a compliant privacy and security notice for CUI.
- Recommend DOD provide guidance regarding a logon banner for CDI for use on an international organization's system and network
- Recommend DOD share all available specifics to include USG or DOD General Counsel federal rules/warnings regarding CDI

3.1.10

- Recommend assessment guidance related to use cases when the function is to always display data

3.1.11

- Recommend assessment guidance regarding locking of the user session, when termination is not possible, due to mission or functionality requirements

3.1.15

- Recommend DOD provide assessment scenarios which need to be explicitly allowed, such as a firewall administrator making firewall changes via a remote session

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

3.1.20

- Recommend adding the method(s) of Policy, Process, and Configuration

3.3.5

- Recommend DOD provide guidelines as to company specification(s) of terms and/or examples to meet the logging requirement
- Recommend DOD provide policy, process, and/or configuration parameters for correlation and audit review to include specification or examples as to the levels of activity regarding indications
- Recommend DOD provide guidance as to assessments regarding small business manual effort comparative to automated application and logging management and reporting system

3.3.6

- Recommend adding guidance for clarity as to the security relevance for on-demand. Assessment criteria for manual processes and on-demand capabilities may differ and may not be technically or operationally feasible to all companies.

3.4.1

- Recommend DOD provide a policy statement and examples or share DOD statements for compliance
- Recommend DOD provide guidance as to small business manual effort in comparison to automated inventory management and reporting system
- Recommend DOD recommend processes for BYOD operations
- Recommend DOD provide the assessment criteria regarding company landscapes across varied enterprises and devices

3.4.8

- Recommend DOD provide guidance on software management resources by specific systems and devices
- Recommend DOD provide guidance or examples of configuration profiles

3.5.3

- Recommend DOD provide a detailed description of the multifactor authentication (MFA) requirement to clarify and specifically state the requirement is transcribed into 4 distinct requirement capabilities (local, privilege, remote access, & internet facing)
- Recommend DOD provide specific information stating the MFA authentication process is enforceable once in the path to access
- Recommend DOD provide guidance as to the MFA requirement applying to Linux, Unix, and varied systems, devices, and services (including cloud)

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

3.5.4

- This capability is typically standard on recent operating systems
- DOD should provide guidance related to an assessment which test or requires detailed information regarding how this control is implemented. Will showing the use of current operating systems meet the requirement? Does the offeror need to provide the specifics of how the operating system implements replay resistant authentication?

3.5.10

- Recommend for assessment clarity that hashing terminology be added for technical criteria consideration

3.7.3

- Recommend minimal thresholds and/or examples of equipment sanitization be added for clarity in assessments

3.7.6

- Recommend the criteria guidance be expanded to include cloud environments

3.8.1

- Recommend adding criteria allowing for buildings with badge/ guard access, and escorting of visitors, be allowed as acceptable for CDI on paper (e.g. 3.10.x requirements)
- Recommend DOD provide guidance related to protection of paper and printing environments
- Recommend minimal thresholds and/or examples of media sanitization be added for clarity in assessments

3.8.4

- Recommend clarity for assessments be added to reference DOD Instruction 5230.24 and include recognition of building boundary protections

3.8.6

- Recommend clarity and guidance regarding physical safeguards and physically secure building boundaries

3.8.7

- Recommend adding Policy/Process to Methods

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

3.9.1

- Recommend assessment clarity regarding the implications if deemed as “Need to Know”
- Recommend DOD provide examples of common screening criteria practices (e.g. enlisted for employment)

3.10.6

- Recommend use cases or scenarios be developed for physical safeguards in comparison to network connectivity/boundaries
- Recommend DOD provide sample policies and procedures as examples for clarification

3.12.2

- Recommend contractor’s/ subcontractor’s POAMs with implementation dates (likely associated with vendor roadmaps) be communicated as being considered compliant. DOD Requiring activities have repeatedly disallowed POAMs

3.12.4

- Request a documented process to understand once a contractor/ subcontractor submits a SSP and associated POAM, the contractor should document from the contracting official regarding the acceptability of the SSP/POAM and a timeframe for when such documentation should be received?
- Regarding prime contractors and higher tiered subcontractors, have they achieved their regulatory obligations to the next tier down when the CDI supplier accepts the contractual document containing the required clauses? If no, what will the contracting official specifically expect from a prime or higher tiered sub for viability, monitoring and assessing their CDI supplier’s information security systems?
- Are suppliers required to share their SSPs/ POAMS with higher tiered subcontractors/primes if there is an expectation for assurance as stated above?

3.13.1

- Recommend examples of internal boundaries to include the associated CDI threats be added for assessment guidance

3.13.2

- How does an offeror “demonstrate/prove” the “standard network designs?”

3.13.3

- Recommend adding clarity as to user roles regarding system management (e.g. end users who have local admin rights)

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

3.13.5

- Recommend the criteria guidance be expanded to include cloud environments

3.13.8

- Recommend alignment and integration of all specifications which vary across DFARS Cybersecurity guides, standards, and FAQ. As an example, Q94: Security Requirement 3.13.8 – When implementing the requirement to “Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards,” is encryption required for a Multiprotocol Label Switching (MPLS) private network (thus an extension of a local network) but it is multi-tenant protected by VLANs? A94: Encryption, though preferred, is not required if using common-carrier provided MPLS, as the MPLS separation provides sufficient protection without encryption.
- Recommend DOD provide clarity and guidance regarding assessment of external transmission and networking boundaries

3.13.9

- Recommend guidance for clarity regarding Local Area Networks exclusion

3.13.11

- Recommend alignment and integration of all specifications which vary across DFARS Cybersecurity guides, standards, and FAQ. As an example, Q68 (Q35/Q36): Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11 – Do all of the 171 security requirements for cryptography have to be FIPS validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient? A68: Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at <http://csrc.nist.gov/groups/STM/cmvp/> and <http://csrc.nist.gov/groups/STM/cmvp/validation.html>. April 2, 2018 43 When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI (or in this case covered defense information). Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

validated cryptography is required whenever the encryption is required to protect CDI in accordance with NIST SP 800-171 or by another contract provision. Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography

3.13.14

- Recommend alignment and integration of all specifications which vary across DFARS Cybersecurity guides, standards, and FAQ

3.13.15

- Recommend guidance on how an offeror does “demonstrate/prove” session protection is implemented. Can an offeror show documentation of the “default configuration” for communications equipment or other systems?

3.13.16

- Recommend DOD provide additional information as to the effect of “at rest” on boundary protections, closed areas, device types, etc.
- Recommend DOD provide additional information on parameters, configuration, or product guidance regarding assessments (i.e. FIPS approved algorithms within the boundary which would be discrepant to Q68 and 3.13.11)

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

Enclosure 2

**ASSESSING THE STATE OF A CONTRACTOR'S INTERNAL INFORMATION
SYSTEM IN A PROCUREMENT ACTION**

INDUSTRY COMMENTS:

OBJECTIVE 1

EVALUATE IMPLEMENTATION OF NIST SP 800-171* AT SOURCE SELECTION

1. This document does not adequately address Cloud.
2. Will DOD assess subcontractor and supplier IT systems that are part of an RFP or contract; such as a joint RFP with a prime, and one or more key subcontractors? If so, how would the overall RFP/contract score be determined?
3. Customer is to identify CUI/CDI. This rarely occurs resulting in prime contractors & subcontractors referring to the CUI Registry and results in excessive CUI/CDI data requirements.

Comments Common to ALTERNATIVES 1A & 1B and OBJECTIVES 2 & 3

1. Requiring prime contractor submittal of SSPs and POAMs as CDRLs will drive additional complexity and oversight, slowing innovation. These are living documents and are ever changing based on the threat environment. When delivered, these documents are only as good as of the time they were printed.
2. With DOD specifying 83% of the controls being high value, the associated evaluation criteria does not provide the necessary differentiation to help contractors prioritize their POAMs.
3. For a large program that could have several suppliers with CDI protection requirements, will there be individual SSPs supplied by all the sub-contractors to the prime or is only the prime SSP supplied? If the requiring activity has not explicitly defined the CDI to be protected, would all sub-contractors that would potentially handle CDI be required to also supply their SSP? It is especially problematic if CDI is not clearly defined in the RFP and the supply chain is included in the evaluation.
4. These alternatives tie program performance criteria to internal IT objectives and project completion. Internal IT would now have to report POAM status to all DOD programs and potentially include in CDRL deliverables. Internal IT would need to be staffed to support BOEs tied to each program.
5. Establishing CUI as a separate technical evaluation factor other than pass/fail will limit/discourage sharing of best practices and erode progress that has been made as part of the DIB and other cross industry groups.

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

ALTERNATIVE 1A

ASSESS NIST SP 800-171* IMPLEMENTATION AS A SEPARATE TECHNICAL EVALUATION FACTOR

1. There needs to be more information on how the DOD will capture these additional requirements (H, M, L). These requirements must remain in an H-Clause in order to most effectively capture the requirements and flow-down when necessary.
2. Clarification is needed regarding whether the evaluation is for the prime system or if it also includes lower tiers. DOD must recognize that Prime Contractors are limited in contract privity to the Tier 1 level of their supply chain only.

ALTERNATIVE 1B

ASSESS NIST SP 800-171* IMPLEMENTATION AS A SEPARATE TECHNICAL EVALUATION FACTOR

1. Security Assurance Levels (which provide a qualitative approach to addressing security for a specific zone or control) can be used to establish the need for additional support due to criticality of the data in procurements.
2. Internal Information Security staffs would need to develop BOEs for every DOD proposal to ensure it is a technical differentiator.
3. What is the scope of “Validate implementation for the competitive range with an independent government assessment in accordance with NIST SP 800-171A...”? Does this mean a solicitation will scan the contractor network, want configuration artifacts, etc.? Will this allow a prime to do this?
4. If solicitations select alternative 1B, does the “assessment” occur before or after contract award? If before how is the cost recovered? Is it a “cost” of participating in a DOD RFP opportunity?
5. What remedies are available if an offeror feels they were unfairly assessed resulting in a poor rating, i.e. does a poor assessment with which a company disagrees warrant a contractual award protest? What remedies are available if an offeror’s IT systems or business is negatively impacted as a result (e.g. as a result of a Penetration test) of an assessment activity? Language from NIST SP 800-171A indicates this could be a possibility. Footnote from Page 69, “¹¹Testing is typically used to determine if mechanisms or activities meet a set of predefined specifications. Testing can also be performed to determine characteristics of a security or privacy control that are not commonly associated with predefined specifications, with an example of such testing being penetration testing.” In most instances, third party assessors performing penetration tests receive indemnification if adverse impacts occur.

Comments Common to OBJECTIVES 2 & 3

1. Protecting CUI with common controls and practices across the enterprise is the most cost-effective solution. Establishing unique protection requirements by

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

program will increase the complexity and therefore cost to protect the information.

2. It is unclear what agency will be evaluating prime contractors. Also, it is unclear what evaluation criteria is to be used.
3. Evaluation of POAMs could vary based on contracts resulting in conflicting priorities for the contractor.

OBJECTIVE 2

REQUIRE PROTECTIONS IN ADDITION TO THE SECURITY REQUIREMENTS IN NIST SP 800-171 AND EVALUATE AT SOURCE SELECTION

1. There is concern that this will introduce requirements outside of the prime contractor. This will be multiplied throughout the supply chain.
2. If each DOD program required protections in addition to NIST SP 800-171, industry could not implement an Enterprise network and each program would essentially be the equivalent of a SCIF in terms of operational support and the associated costs for IT. This would have a dramatic impact on productivity due to the lack of shared tools and processes.
3. Recognize prime contractors are limited to contract privacy at the Tier 1 level of the supply chain. Imposing additional requirements to NIST SP 800-171 controls will result in supply chain issues, due to lack of establishing an industry wide approach."

Comments Common to Both Sections of OBJECTIVE 3

1. This will allow DOD to impose requirements for protecting CUI beyond that of the prime contractor's environment. The risk and complexity increases with the number of sub-contractors.
2. What is the plan for tracking? What is the reporting requirement for the contractor? This may drive additional systems, tools and complexity.
3. "RFP may also identify requirement for periodic reporting of results of continuous monitoring per 800-171 3.12.3." Is the prime responsible for "rolling up" monitoring information from its supply chain that handles CDI? Again, internal IT Security would need to staff for CDRL deliverables.

OBJECTIVE 3

ASSESS/TRACK IMPLEMENTATION OF NIST SP 800-171* SECURITY REQUIREMENTS AFTER CONTRACT AWARD

1. The information necessary for the Government to make an independent assessment is highly sensitive both for security and competitive reasons. How will the Government assure contractors their information will be kept secure? How will this information be transmitted to, stored by, controlled by and destroyed by the Government?

COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS
4401 Wilson Boulevard, Suite 1110
Arlington, Virginia 22203
codsia@codsia.org
www.codsia.org

OBJECTIVE 3

**THE GOVERNMENT MAY ALSO MONITOR COMPLIANCE OF NIST SP 800-171*
WITH INDEPENDENT GOVERNMENT ASSESSMENT**

1. What does support for an independent assessment mean?
2. What mechanisms will be in place to protect the sensitivity of the information provided on SSPs, POAMs and third-party control assessments from a bidder's competitors?"

OBJECTIVE 4

**CONTRACTORS 'SELF-ATTEST' TO COMPLIANCE WITH DFARS 252.204-7012
AND IMPLEMENTATION OF NIST SP 800-171***

1. Companies are still working to fully implement these requirements.