From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comments on NIST SP 800-171r3 Initial Public Draft
Date:	Thursday, July 13, 2023 5:26:14 PM
Attachments:	Tab A - NIST SP 800-171 Rev3 - NIST Comment Matrix - MDA Consolidated Comments.xlsx

Dear NIST,
Attached are NIST SP 800-171 Rev. 3 Draft comments consolidated from the Missile Defense Agency. Please contact Dr. Michael Wojcik at [redacted] is there are any questions.

Best regards,

Michael E. Wojcik, Ph.D.

Missile Defense Agency

ICD DIB Cybersecurity Lead
DA Cyber Advisor

[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Michael Wojcik Ph.D./Missile Defense Agency	Technical	NIST SP 800-171 Rev.3	2	31	Federal Contract Information (FCI) is required to be addressed. FCI is required to be protected with basic safeguarding requirements in the Cybersecurity Maturity Model (CMMC) Level 1. The basic safeguarding requirements are noted in the Code of Federal Regulations (CFR) 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems." The 15 basic safeguarding requirements found in CFR 52.204-21 have been identified as security requirements for FCI in CMMC and need to be denoted with an asterisk in the NIST SP 800-171 Rev.3. Basic safeguarding requirements are identified and applicable to CMMC Level 1 and have corresponding NIST SP 800-171 Rev.3 security requiremets. Since the NIST SP 800-171 Rev.3 is going to be the authoritative security guidance for nonfederal systems and CMMC is the present way for the future FCI is required to be addressed or there will be a loophole in the guidance for the protection of information which includes FCI and CUI.	Federal Contract Information (FCI) is information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government but not including information provided by the Government to the public (such as public websites) or simple transactional information that is necessary to process payments. The security requirements for the protection of FCI are noted by an asterisk which include 3.1.1 3.1.2 3.1.20 3.1.22 3.5.1 3.5.2 3.8.3 3.10.1 3.10.7 3.13.1 3.14.1 3.14.2. Footnote: FCI security requirements are derived from the basic safeguarding requirements found in the Code of Federal Regulations (CFR) 52.204-21 "Basic Safeguarding of Covered Contractor Information Systems."
2	Michael Wojcik Ph.D./Missile Defense Agency	Editorial	NIST SP 800-171 Rev.3	45	1687	Change "control assessments" to read security requirement assessments." This is to stay in line with the NIST SP 800-171 Rev.3 vernacular rather than the NIST SP 800-53 Rev.5 language.	Change to read...."based on the findings from security requirement assessments ...."
3	Alan Booco/Missile Defense Agency	General	NIST SP 800-171 Rev.3	N/A	N/A	Create a user-friendly NIST SP 800-171 Implementation Guide. This would make it easier for small contractors to implement the requirements. Where possible reduce the complexity. Making the document more accessible and easy to understand for non-technical readers.	Example User-Friendly Implementation Guide for the Access Control family. Introduction The Access Control family contains a set of security requirements that are designed to protect sensitive information by controlling who has access to it. The requirements in this family cover a wide range of topic including: -User authentication: This ensures that users are who they say they are before they are granted access to sensitive information -Authentication: This requirement ensures that users only have access to the informatin that they need to do their jobs. -Account Management: This requirement ensures that user accounts are properly created managed and terminated. -Access Control Lists: This requirement ensures that access to sensitive information is contro led by ACLs. -Physical Access Control: This requirement ensures that physical access to sensitive information is controlled. Implementation Guidance The following are some implementation guidance for the Access Control Family: -User authentication: Use a strong authentication mechanism such as multifactor authentication to authenticate users before they are granted access to sensitive information. -Authorization: Use a role-baesd access control (RBAC) system to ensure that users only have access to the information that they need to do their jobs. -Account Management: Create user accounts with strong passwords and expiration dates. Requires users to change their passwords regularly. Disable or delete user accounts that ar eno longer needed. -Physical Access Control: Control physical access to sensitive information by using physical security controls such as locks guards and security cameras. Conclusion: The Access Control family of NIST SP 800-171 Rev.3 contains a set of security requirements that are designed to protect sensitive information by controlling who has access to it. By following the implementation guidance in this section you can help ensure your organization's sensitive information is protected from unauthorized access.
4	Alan Booco/Missile Defense Agency	General	NIST SP 800-171 Rev.3	N/A	N/A	Provide case studies and examples of cost-effective implementations (open-source software and cloud-based services) of specific security requirement to help small contractors. Providing such information would give small contractors a starting point for implementing security measures and would help them avoid wasting resources on ineffective or expensive solutions.	In the Discussion sections for Access Control Audit and Accountability Identification and Authentication Media Protection and Path Management note the possibility of using cloud-based solutions for cost effective implementation. Consider adding case studies for small businesses to see how others have implemented the security requirements while highlighting successes and challenges associated with implementation.
5	Alan Booco/Missile Defense Agency	General	NIST SP 800-171 Rev.3	N/A	N/A	Increase the level of specificity in the security requirements. Making the requirements more clear and unambiguous w ll help small contractors know exactly what is required of them.	The requirement to implement security awareness training could be made more specific by providing topics that should be covered in security awareness training such as phishing social engineering and password management. The requirement to implement security incident response procedures could be made more specific by isting the steps that need to be taken in the event of a security incident such as identifying the incident containing the incident and restoring operations.
6	L Rowbotham MDA/ABJ	Technical	NIST SP 800-171 Rev.3	38	1425	Personnel Termination and Transfer	Under paragrapgh a (When individuals are terminated) an additional action should be to delete or move all CUI files associated with the individual's user account.
7	L Rowbotham MDA/ABJ	Technical	NIST SP 800-171 Rev.3	43	1623	Additional supported format	In addtion to OVAL the Extensible Configuration Checklist Description Format (XCCDF) should be added. Both OVAL and XCCDF are supported by scanning tools (SCAP).