[redacted] [redacted]

**Attachments:** Nickcolus Martin Defense Cyber Security Group sp800-171r3-fpd Comments Jan-26-2024.xlsx

---

---------- Forwarded message ---------
From: Nick Martin [redacted]
Date: Friday, January 26, 2024 at 1:50:12 PM UTC-5
Subject: NIST SP 800-171 Rev. 3 (Final Public Draft) Comments from Nickcolus Martin at DCG
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Dear NIST team,

Please find my comments attached.

Very Respectfully,

Nick Martin

--

**Nickcolus Martin**
Director, Cybersecurity and Information Management
Defense Cybersecurity Group
[redacted]
[redacted] | Web | Social

| Comment # | Submitted By | Type (General | Source (publication, analysis, | Starting Page | Starting Line | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|---|
| 1 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3, Control 03.01.18 | 14 | 424 | The description of mobile devices is not sufficient enough to adequately distinguish smart phones and tablets from small form factor workstation laptops. To address this gap the inclusion of operating system architectural designed for mobile device architecture should be included. For example, mobile devices and their operating systems are designed primarily based on ARM based CPU architecture to optimize untethered wireless operation for extended periods (or almost exclusively) of time. | Provide a more detailed definition of mobile devices that includes the operating system architecture typically used in these devices. This could help businesses better understand which devices fall under this requirement. |
| 2 | Nickcolus Martin/ Defense Cybersecurity Group | General | NIST 800-171r3, Control 03.01.18 | 14 | 439 | The requirement discussion of “conducting primary operating system (and possibly other resident software) integrity checks” is technically challenging without specialized software for mobile device operating systems. For example, a operating system integrity check would require retrieving a copy of the the ISO file from the device via drive cloning which is a highly specialized task requiring a great amount of technical knowledge and tools. Additionally, this would require the OSC to obtain copies of OS updates and security patches from the devices service provider such as AT&T, Verizon, T-Mobile, etc. Would this be required after each update, which could occur multiple times a year? This requirement would be unsustainable for small to medium businesses. | Provide more practical guidance for conducting operating system integrity checks on mobile devices such as anti-virus. |
| 3 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 document, Section 3.2.1. Literacy Training and Awareness | 17 | 533 | In 3.2.1 the requirement to provide security literacy training "On recognizing and reporting indicators" could potentially be interpreted as necessitating training after every threat indicator. The language is vague and could lead to an overburdened training process, particularly for small and medium-sized businesses. The discussion section does not provide sufficient clarity on this point. | Consider using more precise language to clarify the circumstances under which training should be provided. For example, "Provide security literacy training on recognizing and reporting indicators of threats as part of periodic training updates." |
| 4 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 3.3.3 | 19 | 648 | The embedded assessment objective of 3.3.3 a creates a nested requirement that will increase the impact of a NOT MET for the purpose of scoring is SPRS. This effectively makes one assessment objective failure reflect a SPRS score equivalent to several failures. | Consider providing more detailed guidance or examples of adequate logging and review mechanisms suitable for small and medium-sized enterprises. |
| 5 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3, Control 3.3.4 | 20 | 679 | Control 3.3.4 addresses the need for alerting in case of detecting inappropriate or unusual activities. However, the discussion section introduces ambiguity by stating "organizations may decide to take no additional action," which potentially undermines the effectiveness of the control. | Revise the discussion text to clarify the importance of taking action upon receiving alerts of inappropriate or unusual activities or provide an ODP of what may be defined as a threshold to alerting. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 3.3.4 | 20 | 669 | The discussion section of requirement 3.3.4 could benefit from more explicit language and examples to help small and medium-sized businesses understand the implications of different types of audit logging process failures. For example, "Organizations may decide to take no additional actions after alerting", but above examples of response actions are given starting at line 671. Are those actions the minimum actions that are in fact required, or may an organization simply implement no response? If the later is the case Assessment Objective B should be revoked. | Include more explicit language and examples in the discussion section and note the examples as minimum requirements to meet AO B or revoke AO B. |
| 7 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 3.3.5 | 20 | 685 | Requirement 3.3.5 emphasizes the importance of frequent review, analysis, and reporting of system audit records. However, for small and medium-sized businesses, the requirement to "analyze and correlate audit records across different repositories to gain organization-wide situational awareness" might be challenging due to potential resource constraints and lack of technical expertise. Furthermore, the term "organization-wide situational awareness" is a broad scope that may not include CUI systems and is out of the bounds of requirements of DFARS 7012. This creates a requirement that would impact none CUI systems which in turn is out of scope of 800-171. | Provide more explicit guidelines or examples on how to analyze and correlate audit records across different repositories. Further, refine the scope of "organization-wide situational awareness" to focus specifically on systems handling CUI to align with the requirements of DFARS 7012. |
| 8 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 3.3.5 | 20 | 692 | The discussion section of requirement 3.3.5 will benefit from more explicit language and examples to help small and medium-sized businesses understand the scope of audit record review, analysis, and reporting. The requirement should also provide an organization-defined parameter (ODP) for "unusual activity". Without the ability to create an ODP for unusual activity it provides the assessor the ability to determine activity, that may be normalized for the organization, but can be interpreted, without evidence, as suspicious activity. For example some vehicles have wifi scanning modes that will be detected by a business next to a highway. This may be suspicious activity that an organization can do little to prevent. While the security of the wifi network is unaffected this can be considered suspicious by an outside party. | Include more explicit language and examples in the discussion section. For instance, provide examples of what constitutes "inappropriate or unusual activity", and give examples of how to adjust the scope, frequency, and depth of the audit record review, analysis, and reporting to meet organizational needs. Additionally, introduce an ODP for "unusual activity" to help organizations identify and respond to potential threats |
| 9 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 3.3.6 | 21 | 710 | Requirement 3.3.6 example given in the discussion, which mentions the use of "modern data mining techniques with advanced data filters to identify anomalous behavior in audit records," implies the need for advanced Security Information and Event Management (SIEM) tools. For small and medium-sized businesses, this would significantly increase cost and complexity. This requirement is a substantial escalation from what was stipulated in revision 2, and many organizations may not have the resources or expertise to implement such advanced tools. While the use of a SIEM is crucial for proper incident response, the ongoing requirement for advanced filtering and custom reporting may be too extreme for many businesses. | Reconsider the requirement for advanced data mining techniques and advanced data filters. Instead, provide more realistic and achievable examples and guidelines for audit record reduction and report generation. The focus should be on effective incident response methods, which can be achieved with standard SIEM tools. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 10 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 3.4.1 | 22 | 771 | Requirement 3.4.1 lacks clarity on the definition of "system baseline" and what components it should include. The requirement should provide an organization-defined parameter (ODP) where the organization can specify what is included in their system baseline. For instance, it's unclear whether software, outside of Operating Systems and firmware, is included in this scope. Including such software in the baseline configuration could significantly increase the management burden for many businesses, making it unattainable. | Clarify the definition of "system baseline" and specify what it should include. Introduce an ODP where organizations can define what is included in their system baseline. Consider explicitly stating that software, outside of Operating Systems and firmware, is not required to be included in the system baseline. |
| 11 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 3.4.3 | 23 | 821 | The requirement in assessment objective B for a security engineer to conduct a formal security impact analysis similar to NIST 800-53 could be burdensome for a significant portion of the Defense Industrial Base, particularly for smaller organizations. Conducting a formal security impact analysis requires specialized knowledge and can be time-consuming. Many smaller organizations in the DIB may lack the resources to carry out this requirement effectively. | Consider providing additional guidance or resources to help organizations carry out a security impact analysis effectively. This could include simplified guidelines, tool recommendations, or examples of best practices. Alternatively, consider adjusting the requirement to better align with the resources and capabilities of smaller organizations. |
| 12 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 3.4.4 | 24 | 836 | Requirement 03.04.04 for analyzing the security impact of changes to the system prior to implementation seems redundant given the requirement of a security impact analysis is already imposed by 3.4.3 b. While the further guidance in this section is an improvement to 3.4.3 b, the increase in scope to include the supply chain is overly burdensome, particularly for small and medium-sized businesses within the Defense Industrial Base. | Consider rolling this control into further guidance for 3.4.3b and striking the language around "supply chain" impact analysis. This would reduce redundancy and make the requirements less burdensome for organizations, particularly smaller organizations. |
| 13 | Nickcolus Martin/ Defense Cybersecurity Group | General | NIST 800-171r3 3.4.5 | 25 | 866 | Requirement 03.04.06 is a positive change that improves on the guidance provided in 800-171 rev 2. It better establishes guidelines for organizations, particularly small and medium-sized businesses within the Defense Industrial Base, to configure their systems to provide only mission-essential capabilities and to prohibit or restrict use of certain functions, ports, protocols, connections, and services. This change is recommended to be kept. | No change suggested. |
| 14 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 3.4.8 | 26 | 895 | The discussion within requirement 03.04.08 is comprehensive and provides valuable guidance. However, there seems to be a discrepancy between the language in the discussion and the language in Assessment Objective B. This inconsistency reduces the usefulness of the discussion and may cause confusion for small and medium-sized businesses within the Defense Industrial Base. This discrepancy will cause organizations to fail an assessment given the strict language in AO B. | Revise the language in Assessment Objective B to be more flexible and in line with the discussion. This would make the requirements more consistent and easier to understand and implement. |
| 15 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST SP 800-171r3 3.4.11 | 27 | 945 | Requirement 03.04.11 for identifying and documenting the location of CUI and the system components on which the information is processed and stored seems to overlap with the system component inventory requirement (03.04.10). Both requirements involve documenting and tracking system components, which could lead to duplication of effort. | I recommend striking 3.4.11 a since this is already satisfied by 3.4.10. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 16 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3, 3.4.12. System and Component Configuration for High-Risk Areas | 27 | 974 | The requirement specifies the sanitation of hard drives prior to going into high-risk areas. However, if no Controlled Unclassified Information (CUI) is present within the system, then it is not in scope of NIST 800-171 and no further controls are required. If a device that has previously been out of the system then system configuration baseline and other controls within this control family would apply. This control seems redundant and appears to increase documentation burdens and requirements without adding significant security value. | Clarify the necessity of this requirement in the context of systems without CUI. If the requirement is indeed redundant, consider removing it or merging it with other similar requirements to reduce the documentation burden. |
| 17 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3, 3.5.4. Replay-Resistant Authentication | 29 | 1033 | Requirement 3.5.4 mandates the implementation of replay-resistant authentication mechanisms for access to system accounts. While this is a crucial security measure, the technical complexity of implementing such mechanisms could be a significant challenge for small and medium businesses. However, this control appears to be redundant as it is covered by 3.5.3. Multi-Factor Authentication and 3.5.2. Device Identification and Authentication, which includes technologies like PKI that are inherently resistant to replay attacks. An example of a technology that fulfills this requirement is Time-based One-Time Password (TOTP) MFA. | Provide more specific guidance on cost-effective and less technically complex replay-resistant authentication mechanisms suitable for small and medium businesses. This could include a list of recommended solutions and a step-by-step guide on how to implement them. Also, consider merging this requirement with 3.5.3 and 3.5.2 to reduce redundancy. |
| 18 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3, 3.5.4. Replay-Resistant Authentication | 30 | 1033 | Requirement 3.5.4 on Replay-Resistant Authentication appears to be redundant as it is already covered by 3.5.3. Multi-Factor Authentication and 3.5.2. Device Identification and Authentication. Both of these controls involve technologies, such as Public Key Infrastructure (PKI) and Time-based One-Time Password (TOTP) Multi-Factor Authentication (MFA), that are inherently resistant to replay attacks. | Consider merging this requirement with 3.5.3 and 3.5.2 to reduce redundancy and simplify the implementation process for small and medium businesses. Provide clear examples and guidance on how technologies like PKI and TOTP MFA provide replay-resistant authentication. Additionally, I would recommend providing more definitive guidance based on NIST SP 800-63b under subsection 5.1.3.1 Out-of-Band Authenticators. |
| 19 | Nickcolus Martin/ Defense Cybersecurity Group | Technical | NIST 800-171r3 document, Section 3.5.7. Password Management | 31 | 1066 | Requirement 3.5.7b, which involves verifying new or updated passwords against a list of commonly-used, expected, or compromised passwords, significantly increases the need for third-party tools like centralized password management services. This could substantially increase the complexity of deployment requirements for small and medium-sized businesses. Furthermore, while NIST 800-171 doesn't directly correlate with DFARS and CMMC, this requirement implies that organizations may need to use FedRAMP ATO'ed services for centralized password management. This could potentially limit the use of common tools like "Have I Been Pwned", which could otherwise be used to satisfy this requirement. | Additional consideration about imposing 3.5.7 (b) as a reasonable measure. The difficulty in implementing tools to satisfy this requirement is immense and other more effective methods could be employed, such as a recommendation within the discussion to for the use of random password generators, which are much more ubiquitous and could be deployed easily within an organizations boundary. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 20 | Nickcolus Martin/ Defense Cybersecurity Group | Editorial | NIST 800-171r3 document, Section 3.5.11. Authentication Feedback | 33 | 1097 | While the requirement to obscure authentication feedback is generally addressed by most technologies through text field obfuscation using programing libraries such as getPass and bCrypt, 3.5.11 does not address the importance of procedural security. It is crucial for users to have situational awareness during the authentication process to prevent threats such as 'shoulder surfing' which can also compromise passwords based on keyboard input. | It is recommend adding a discussion item that emphasizes the importance of procedural security and user awareness during the authentication process. This could be included in the discussion within Awareness and Training. |
| | | | | | | | |
| | | | | | | | |