| | |
|---|---|
| **From:** | [redacted] via 800-171comments |
| **To:** | 800-171comments@list.nist.gov |
| **Subject:** | [800-171 Comments] Submission of GSA Comments on Enhanced Security Requirements for Protecting Controlled Unclassified Information |
| **Date:** | Friday, January 10, 2025 12:16:14 PM |
| **Attachments:** | sp800-172r3-ipd-comment-template.xlsx |

Dear NIST Team,

I hope this message finds you well. On behalf of the General Services Administration (GSA), I am submitting our comments on the recently released request for public input regarding the Enhanced Security Requirements for Protecting Controlled Unclassified Information (CUI). We appreciate the opportunity to provide feedback on these important security requirements.

Attached to this email is a spreadsheet that includes our comments, suggestions, and any clarifications that we believe could contribute to enhancing the framework. We have carefully reviewed the proposed requirements and look forward to further collaboration as these guidelines evolve.

Please do not hesitate to contact me if you require any additional information or clarification regarding the attached comments.

Thank you for considering GSA's input, and we look forward to continued engagement on this important issue.

Best regards,

**U.S. General Services Administration**

**Anthony Miller,** FAC-P/PM / FAC-COR / CSM
IT Security Division (ITSD)
Risk Management and Analysis Support Services (RMASS)
Information Technology Category (ITC)
Federal Acquisition Service (FAS)
[redacted]

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Starting Page # * | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|---|---|---|---|---|---|---|
| 1 | GSA/FAS/ITC/ITSD/RMASS | Editorial | 5 | 311 | Although the enhanced security requirements are derived from the security controls and control enhancements in SP 800-53, which addresses 20 security control families, only 17 of these security control families are selected in this SP 800-172 and SP 800-171 Rev 3. | Recommend explaining the reason three (3) SP 800-53 control families are not selected for this SP 800-172: Assessment, Authorization, and Monitoring (CA); Physical and Environmental Protection (PE), and Program Management (PM). |
| 2 | GSA/FAS/ITC/ITSD/RMASS | Editorial | 6 | 332 | Table 1. Enhanced security requirement families | Recommend including family acronyms and bookmark/link the acronym to the corresponding two-digit section. This convenience will be appreciated by the reader. |
| 3 | GSA/FAS/ITC/ITSD/RMASS | Editorial | 6 | 338 | ODPs are introduced but not defined. "Organization-defined parameters (ODPs) are used in certain enhanced security requirements. ODPs provide flexibility through the use of assignment and selection operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements. " | ODPs should be defined here. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | GSA/FAS/ITC/ITSD/RMASS | Technical | 7 | 362-366 | Section 3 The Requirements, enhanced security requirements, lists the source controls from SP 800-53 associated with the enhanced security requirement. The security control requirements in this SP 800-172 maps to the SP 800-171 security control requirements. However, the referenced source controls in this SP 800-172 do not always match the source controls listed in the SP 800-171. For example: SP 800-172 03.01.02E shows source control AC-20(03) and enhances SP 800-171 requirement 03.01.20. SP 800-171 03.01.20 shows source controls AC-20, AC-20(01), and AC-20(02) (not AC-20(03). A valid reason for not exactly matching probably exists and should be explained. | For clarity, explain why the referenced source controls in this SP 800-172 do not always match the source controls listed in the SP 800-171. |
| 5 | GSA/FAS/ITC/ITSD/RMASS | Techncial | 9 | 399 | Consider adding the Assessment, Authorization, and Monitoring (CA) control family. This family includes controls that can provide enhanced security requirements aimed at protecting the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) in nonfederal systems and organizations. These enhanced security requirements are designed to support a range of protection strategies, including deterring, delaying, or detecting adversarial actions. | The Assessment, Authorization, and Monitoring (CA) control family primarily focuses on the oversight of information systems and includes controls that ensure continuous monitoring, security assessments, and authorization processes. Enhanced security requirements in this family can contribute to the protection of CUI by:<br><br>• Implementing continuous monitoring practices to promptly identify and mitigate potential threats to confidentiality, integrity, and availability.<br>• Establishing advanced authorization mechanisms to ensure that only approved systems and individuals can access CUI.<br>• Utilizing automated and manual assessment techniques to detect and respond to vulnerabilities that adversaries might exploit.<br><br>Enhanced security requirements might be found in the following control examples:<br><br>• CA-2 Control Assessment): Enhanced assessments might involve more frequent or deeper reviews of system configurations and vulnerabilities.<br>• CA-7 Continuous Monitoring: Advanced monitoring techniques, such as automated threat detection and real-time reporting.<br>• CA-8 Penetration Testing: Performing regular, sophisticated penetration tests to identify and mitigate potential vulnerabilities. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | GSA/FAS/ITC/ITSD/RMASS | Technical | 9 | 399 | Consider adding the Program Management (PM) control family. This family includes controls that can provide enhanced security requirements aimed at protecting the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) in nonfederal systems and organizations. These enhanced security requirements are designed to support a range of protection strategies, including deterring, delaying, or detecting adversarial actions. | Program Management controls address the overarching governance and risk management of information security programs within an organization. Enhanced security requirements related to this family can include:<br><br>• Establishing comprehensive policies that emphasize the importance of protecting CUI.<br>• Creating an incident response program that ensures timely detection and response to incidents that could compromise CUI.<br>• Developing a robust risk management strategy that includes adversary modeling and balancing protection strategies across prevention, detection, and response capabilities.<br><br>Enhanced security requirements might be found in the following control examples:<br><br>• PM-8 Critical Infrastructure Plan: Developing plans that incorporate advanced threat models specific to protecting CUI.<br>• PM-11 Mission/Business Process Definition: Integrating detailed security considerations into mission and business processes to protect CUI.<br>• PM-16 Threat Awareness Program: Establishing a program that provides advanced threat awareness training and strategies to employees.<br>• PM-30 (Supply Chain Risk Management Strategy): Involves establishing and maintaining a supply chain risk management strategy that addresses risks to the organization's supply chain, including components related to CUI protection. |
| 7 | GSA/FAS/ITC/ITSD/RMASS | Technical | 9 | 399 | Consider adding the Personally Identifiable Information Processing and Transparency (PT) control family. This family is intended to protect PII processed in nonfederal systems. | For effective protection against the loss and degradation of the PII data, the following list of PT controls require appropriate measures to prevent, delay, or intercept unauthorized access to and/or use of the information processing.<br>Key measures include:<br>• Controlling access to systems handling PII.<br>• Implementing encryption and other data protection technologies.<br>• Establishing clear policies and procedures for data processing transparency.<br>This category encompasses such PT controls as:<br>• PT-1: Policies and procedures for PII processing.<br>• PT-2: Who is authorized to process PII and the extent of the authority.<br>• PT-3: Recording facts for which it is intended to use PII.<br>• PT-4: Seeking approval of a subject to allow their PII to be processed.<br>• PT-5: Fairly informative privacy declarations.<br>• PT-6: System of records notices as per the law. |
| 8 | GSA/FAS/ITC/ITSD/RMASS | Technical | 81 | 2711 | Consider adding the definition of "organizational system" in Appendix B. Glossary. | Definition and scope of the terms "organizational system" is crucial for applicability. In some sections, additional examples or clearer distinctions between organizational system components would help interpret these requirements more uniformly. |
| 9 | GSA/FAS/ITC/ITSD/RMASS | Technical | 84 | 2804 | Appendix C's mapping to SP 800-53 controls could include more detailed cross-referencing for organizations using multiple compliance frameworks. This may assist in practical adoption without redundant efforts. | Expanding this mapping to include more detailed cross-referencing with other major frameworks (e.g., ISO/IEC 27001, CMMC, HIPPA, PCI DSS, GDPR, or industry-specific regulations) would significantly benefit organizations that need to comply with multiple standards simultaneously. |

| | | | | | | |
|---|---|---|---|---|---|---|
| 10 | GSA/FAS/ITC/ITSD/RMASS | Technical | 84 | 2804 | *Section 3 The Requirements*, enhanced security requirements, references the SP 800-171 requirement being enhanced (e.g., "This requirement enhances SP 800-171 requirement 03.04.01."), where applicable. *Section 3 The Requirements*, enhanced security requirements, also references the SP 800-53 source control (e.g., SC-26). However, this information is not shown in the *Appendix C Table 2. Enhanced security requirements*. Displaying this information would strengthen the understanding of the requirement mapping. | Recommend the *Appendix C Table 2. Enhanced security requirements* also include the Section 3 SP 800-171 requirement being enhanced and the SP 800-53 source control shown in Section 3. |
| 11 | GSA/FAS/ITC/ITSD/RMASS | Techncial | 93 | | NIST should consider defining the Organization-Defined Parameters (ODPs) in Appendix E, or at least providing recommended default values, based on established NIST guidance. | This would ensure enhanced security requirements are consistently applied to protect the confidentiality, integrity, and availability of Controlled Unclassified Information (CUI) within nonfederal systems and organizations. By specifying baseline or example ODPs, organizations can better align with the high standards required for safeguarding sensitive information, minimizing ambiguity in implementation and supporting a more uniform approach across entities handling CUI. This would enhance both compliance efforts and operational security strategies. |
| | | | | | | |
| | | | | | | |