From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Subject: [800-171 Comments] comments-NIST SP 800-172 Rev. 3 (Initial Public Draft)
Date: Sunday, January 12, 2025 1:30:38 PM
Attachments: nistsecrulemb11225.pdf

Good afternoon: please find attached my comments on NIST SP 800-172 Rev 3 (initial public draft). Please note that these comments reflect solely my personal views and not those of an agency or organization...Thank you, Mitchell Berger

---

The public comment period is open through January 10 January 17, 2025. NIST strongly encourages you to use the comment template and submit comments to 800-171comments@list.nist.gov. Comments received in response to this request will be posted on the Protecting CUI project site after the due date. Submitters' names and affiliations (when provided) will be included, while contact information will be removed.

To: Ron Ross (NIST), Victoria Pillitteri (NIST)
From: Mitchell Berger, (comments made in personal capacity), [redacted]
1.12.2025
Re: Enhanced Security Requirements for Protecting Controlled Unclassified Information, https://csrc.nist.gov/pubs/sp/800/172/r3/ipd

Dear Mr. Ross and Ms. Pillitteri: I write to briefly comment on the above document with the following considerations and suggestions:

Discuss distributed/immutable/ephemeral approach rather than confidentiality, integrity and availability (CIA): Some security experts view the "CIA" approach as outdated, urging instead urging focus on 'distributed, immutable or ephemeral approach' which focuses more on design of a system than the information itself.[1] The CIA approach is discussed several times in the draft SP (pages 2, 4 9) and NIST may wish to consider if a distributed/immutable/ephemeral approach complements this strategy.

Include permanent US Residents (i.e., Green Card holders): Section 03.09.04E Citizenship Requirement discusses "Verify[ing] that individuals accessing a system processing, storing, or transmitting CUI are U.S. citizens." I suggest that lawful permanent US residents, also known as Green Card holders, be included.[2] As of Jan. 2024, the Department of Homeland Security reported that there were roughly 12.8 million lawful permanent residents.[3]

Make recommendations for Penetration Testing more nuanced (Section 03.12.01E): Penetration testing tends to be costly and require outside expertise.[4] In some cases, such testing may not be required and automated vulnerability assessments may be sufficient. In other cases, steps beyond typical penetration testing may be appropriate such as ethical hacking and red teaming.[5] Perhaps this could be discussed as a continuum with factors to guide when a higher level of scrutiny is needed (such as those dealing with health information or organizations with a history of cyberthreats). In the current draft the recommendation ("Conduct penetration testing") seems to be that all organizations are expected to use penetration testing. Thank you for your consideration of this input.

Sincerely,

Mitchell Berger Note/Disclosure: I am submitting these suggestions solely in my personal/private capacity. The views expressed are mine only and should not be imputed either to other individuals or to any public or private entity.

[1] https://medium.com/@marioplatt/threat-modelling-in-a-post-c-i-a-world-focus-on-d-i-e-964c9c29358; https://www.rsaconference.com/library/presentation/usa/2021/death-to-cia-long-live-die-how-the-die-triad-helps-us-achieve-resiliency; https://www.techtarget.com/searchsecurity/feature/Experts-say-CIA-security-triad-needs-a-DIE-model-upgrade
[2] https://www.uscis.gov/green-card; https://ohss.dhs.gov/topics/immigration/lawful-permanent-residents/profiles-lawful-permanent-residents
[3] https://ohss.dhs.gov/sites/default/files/2024-11/2024_1108_ohss_lawful_permenent_resident_population_estimate_2024_and_revised_2023.pdf
[4] https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/;https://www.securitymetrics.com/blog/how-much-does-pentest-cost
[5] https://www.indusface.com/blog/how-penetration-testing-is-different-from-ethical-hacking/;https://www.securitymetrics.com/blog/pentesting-vs-vulnerability-scanning-whats-difference; https://www.sentinelone.com/blog/the-realm-of-ethical-hacking-red-blue-purple-teaming-explained/