

Frank Smith

Jan 15, 2026, 8:33:26 AM

to 800-171comments@list.nist.gov,

Attached are combined comments from the SEI and JHUAPL on NIST SP 800-172 r3 FPD and NIST SP 800-172A r3 IPD

Please let us know if you have any questions.

v/r

Frank

Frank Smith, CISSP

Cybersecurity Team Lead

CERT Division

Phone: Mobile:

| Comment # | Submitted By (Name/Org):* | Type (General / Editorial / Technical) | Starting Page #* | Starting Line #* | Comment (include rationale)* | Suggested Change* |
|-----------|---------------------------|--|------------------|------------------|---|--|
| 1 | APL/SEI | General | 18 | 686 | Title says "literacy training" and objectives say "security literacy training"; the latter is more clear as to intent | Change title to "Advanced Security Literacy and Awareness Training" |
| 2 | APL/SEI | General | 19 | 715 | Same as above; recommend "security literacy" instead | Change title to "Security Literacy and Awareness Training Practical Exercises" |
| 3 | APL/SEI | General | 22 | 804 | ODPs 01 and 02 reference 03; would make more sense to already have 03 defined before the ODPs that reference them | Re-order ODPs so that the current 03 is first |

| | | | | | | |
|---|---------|-----------|----|------|---|--|
| 4 | APL/SEI | Editorial | 25 | 885 | Missing } | A.03.04.02E.ODP[02]: one or more of the following PARAMETER VALUES is/are selected: {disable network access by unauthorized or misconfigured system components; isolate unauthorized or misconfigured system components; notify <A.03.04.02E.ODP[03] personnel or roles>. } |
| 5 | APL/SEI | General | 26 | 924 | Separate ODPs for currency, accuracy, and completeness are not needed as a single mechanism would be typically used | A.03.04.03E.ODP[01]: automated mechanisms used to maintain the currency, completeness, and accuracy of the system component inventory are defined. DELETE A.03.04.03E.ODP[02] and[03] |
| 6 | APL/SEI | Technical | 31 | 1091 | New verbiage loses "replay resistant." Adding it back in. | A.03.05.01E: <A.03.05.01E.ODP[01]: devices and/or types of devices> are authenticated before establishing a system connection using bidirectional authentication that is cryptographically based and replay resistant . |
| 7 | APL/SEI | General | 48 | 1634 | 172r3FPD uses "cyber threat-hunting" while 172ar3IPD uses "cyber threat" Also on lines | A.03.11.02E.a.01[01]: a cyber threat- hunting capability is established to search for indicators of compromise in organizational systems. |

| | | | | | | |
|---|---------|-----------|----|------|--|--|
| | | | | | 1636,1638, 1640 | |
| 8 | APL/SEI | Editorial | 58 | 1953 | Spelling "employedd" | employed |
| 9 | APL/SEI | Editorial | 68 | 2294 | Text says "separate physical or logical domains" but it can also be a combination of the two | Change text to "separate physical and/or logical domains" |