From:	[redacted] via 800-171comments
To:	800-171comments@list.nist.gov
Subject:	[800-171 Comments] Comment Submission: NIST SP 800-172 Rev. 3
Date:	Thursday, January 16, 2025 1:40:18 PM
Attachments:	NIST SP 800-172 Rev. 3 Initial Public Draft_HPE Response.xlsx

---

HPE appreciates the opportunity to comment on the NIST SP 800-172r3 Enhanced Security Requirements for Protecting Controlled Unclassified Information Initial Public Draft. Comments for the draft specification are included in the attached NIST provided content template. We will gladly answer any questions during your review.

Please acknowledge receipt of this email.

Thank you,
Alex King
Hewlett Packard Enterprise

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Hewlett Packard Enterprise (HPE)	Technical	9	420	The 03.01.01E control is titled "Dual Authorization for Commands and Actions" however the discussion section says this requirement should be for privileged commands, not unprivileged. If all commands and actions, including unprivileged actions by end-users, were required to be protected by dual authorization, it could create undue latency in being able to maintain the operation of a system. This could potentially lead to undesirable workarounds being implemented by users or administrators. The ability to practice dual authorization is limited by the number of privileged administrators, of which in some systems there can be one or a small few. In addition, Change Control requirements in NIST SP 800-171 already require any changes to the operating or designed state of the system be reviewed, recorded, and approved before being made. These change control requirements, if adhered as written, require that no changes or commands are run without approval. In certain system down severity 1 scenarios, enforcing dual authorization for every command and action could increase down time due to increasing a longer Mean Time To Repair (MTTR). Although there are third-party enterprise solutions, which partially provide a dual-authorization functionality, if this control is for an OS command level, there are very limited methods to meet this control. One is from a third-party open-source module called Sudo pair, which can be used to meet this control but is only usable for privileged commands requiring the actor be in the sudoers file. Unrelated, we assert that any command or action for which dual authorization would be considered necessary should always require elevated privilege such as being a member or the sudoers group.	The title of the control should include the clarifying word "privileged" in the title such that it says, “Dual Authorization for Privileged Commands and Actions.” This will match the discussion section that includes the qualifier of “privileged.” This will ensure the requirement is limited to privileged actions such as potentially negatively impacting actions, and not everyday commands or actions performed by end users. It is also of far more importance to ensure that dual authorization is required when permissions or access management changes for entities and/or resources are changed. This helps ensure any compromised privileged account cannot be used by a bad actor to give themselves a hidden unauthorized backdoor account that can be hard to detect and track.

2	Hewlett Packard Enterprise (HPE)	Technical	12	510	The 03.01.07E control is titled “Automated Actions for Account Management” and line 512 includes the scope of account disabling and account removal actions. However, the discussion section details this being used for audit purposes only. If this is intended as an audit log or audit reporting only requirement, the word “Auditing” should be the second word of the title. The referenced 800-53 controls explicitly include audit in the title.	There are other industry-specific compliance controls that can require automatic disabling and/or removal of accounts that this requirement could be implying. Some examples of this include removing a user’s access automatically after they are no longer employed, a member of the same organization, when a user’s role has changed, or when a user has not logged in for 30 days. The NIST SP 800-53 controls, which this requirement comes from in the reference, is explicitly limited to audit, thus the title should be “Automated Auditing of Account Management Actions.” However, if the intent is to require more than automatic auditing of account management activity, and require automatic actions being taken such as disabling or removing access for a user, the discussion section should be modified to include more than audit logging and/or reporting to include removal, as an example. Of note: the spec does not include any access revalidation period requirement control.

3	Hewlett Packard Enterprise (HPE)	Technical	21	778	To ensure NIST can securely monitor inventory of a system post-installation, NIST needs to maintain historic versioning of the system component inventory even at an element or component level. Not including inventory version history can lead to errors in inventory, as well as stability and security issues if only the original inventory of the hardware and/or software components change over time. For example, a resource used by one protected workload is later given up by that workload and used by a second workload with different data protection and access permissions. Without tracking awareness, the owner of a resource changed, and the system may leak privileged information from one workload to another workload or a new admin or user who was not authorized for access to the information. This can include not only data on disk but inventory metadata such as IPs, name, and more. Even allowing a new component owner or resource owner to read metadata in an inventory could be a potentially serious information disclosure violation. Another example of the need for inventory versioning is public IP inventory history where a bad actor could have previously used a public or internal IP in a bot or DoS/DDoS network or other malicious action, for which an abuse report was received when the IP was allocated to a previous owner and not the current owner of the IP. In those scenarios you do not want to abandon the IP entirely, so you need the inventory history of that IP to know whether it is still used by a bad actor or if it has been reclaimed and safe to re-allocate to another workload.	Add a third sentence that conveys a requirement that inventory information needs to include historic versioning of the information to track the changes in inventory and its ownership over the lifecycle of the system component inventory.

4	Hewlett Packard Enterprise (HPE)	General	48	1648	The randomization of storage locations may introduce significant complexity for dubious advantage. It may be helpful to add an example where it has been implemented to fairly good effect. The only one that comes to mind is kernel address space layout randomization, which is addressed under “03.14.14E Memory Protection.” This requirement is focused on non-volatile long-term storage, so a more relevant example would be best.	Add an example to the text.
5	Hewlett Packard Enterprise (HPE)	General	15	615	Since training improves the awareness of unrealized exploitation, Adversary Effects should include Expose (Reveal).	Preclude (Preempt), Expose (Detect, Reveal)
6	Hewlett Packard Enterprise (HPE)	General	16	631	Not only detecting the vulnerable area through the simulated threat, but training improves the awareness of unrealized exploitation; Adversary Effects should include Expose (Reveal).	Preclude (Preempt), Expose (Detect, Reveal)
7	Hewlett Packard Enterprise (HPE)	General	17	649	Since training improves the awareness of unrealized exploitation, Adversary Effects should include Expose (Reveal).	Preclude (Preempt), Expose (Detect, Reveal)
8	Hewlett Packard Enterprise (HPE)	General	24	892	Cryptographic does not guarantee perfect secrecy, it just takes longer to break the cipher based key size. Thus, Impede (Exert) should be added as part of the Adversary Effects.	Preclude (Preempt, Negate), Impede (Exert), Expose (Detect)
9	Hewlett Packard Enterprise (HPE)	General	25	930	Device attestation could also detect the malicious component added by Adversary. Thus, Expose (Detect) should be added as part of the Adversary Effects.	Preclude (Preempt), Impede (Exert), Expose (Detect)
10	Hewlett Packard Enterprise (HPE)	Editorial	27	984	Security Operations Center (SOC) should be capitalized.	Security Operations Center (SOC)
11	Hewlett Packard Enterprise (HPE)	General	28	1003	SOC helps propagation of the incidents and threat vector to other communities; thus, Expose (Reveal) is also added to the Adversary Effects.	Limit (Shorten, Reduce); Expose (Detect, Reveal)