[redacted]

[redacted]
From: R. Ikuenobe Osolease [redacted]>
Date: Tuesday, December 10, 2024 at 10:00:42 AM UTC-5
Subject: Enhanced Security Requirements for Protecting Controlled Unclassified Information (Comments)
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Morning,

Please see the comments attached.

Rich

R. Ikuenobe Osolease, Ph.D, CISSP-ISSMP

RGB Professional Services LLC

[redacted]

[redacted]

[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	Dr. Rich Osolease / RGB-PS LLC	Technical	9	420	Unlike Federal agencies, small organizations may lack the personnel to implement dual authorization, making this requirement resource intensive.	Enhancement 03.01.01E implies the need for two technical administrators at the keyboard. The discussion should expand to include "processes such as a change control board (CCB)," whereas an initial authorization of a technical director provides approval before the actual technical changes made.
2	Dr. Rich Osolease / RGB-PS LLC	Technical	10	439	Small businesses may lack centralized controls to enforce all restrictions on non-organizational devices as discussed in the enhancement discussion.	Enhancement 03.01.02E implies there is a need to determine what hardware to restrict processing CUI. The enhancement should also include some mandatory reporting capability, consistent with data owners' reporting requirement other incidents of breach, and formal incident reporting. Reporting should be a part of the restriction control.
3	Dr. Rich Osolease / RGB-PS LLC	Technical	11	480	Automated monitoring tools can be costly, and small businesses may not have the technical expertise to manage and analyze remote access.	Enhancement 03.01.05E implies the mandatory deployment of "automated" monitoring tools like cloud-based remote access monitoring and enable basic logging through firewalls and VPNs. The discussion should specifically define the intent of "automated," and explicitly avoid the use of manual processes. The enhancement description should focus more attention on automation.

4	Dr. Rich Osolease / RGB-PS LLC	Technical	13	580	Advanced access control models may not align with the simpler operational structures of small businesses. Seeking flexibility over uniformity with agency requirements.	Enhancement 03.01.09E implies attribute-based (ABAC) should be use instead of traditional control by subjects and object for access control and use attributes, but don't provide guidance or flexibility to start with less costly but just protective approach such as with role-based access control (RBAC) and then allow the organization to gradually move toward attribute-based access as needed, leveraging existing low-cost software. Consider changing this enhancement requirement allowing the flexibility of RBAC and movement towards ABAC.
5	Dr. Rich Osolease / RGB-PS LLC	Technical	15	589	Small businesses often lack resources to fund comprehensive advance training programs or employ specialized trainers.	Enhancement 03.02.01E implies the need to increase cybersecurity literacy for advanced persistent threats (APTs), indicators of anomalous behaviors, and security literacy training. Non-federal organizations should have access to the same quality and content of Federal training as baseline then follow up with industry specific literacy training using free or low-cost training platforms like security and Infrastructure Security Agency (CISA) resources for awareness programs.
6	Dr. Rich Osolease / RGB-PS LLC	Technical	17	662	Maintaining separate storage environments for audit records may require additional infrastructure not affordable for small businesses.	Enhancement 03.03.01E implies the need for separated computing and storage environments of audit records. Physical separation is required. The discussion should explicitly state that logical separation is not enough.

7	Dr. Rich Osolease / RGB-PS LLC	Technical	20	746	Automation tools for misconfiguration detection are often expensive and may not be feasible for small businesses with limited budgets.	Enhancement 03.04.02E implies the need to use open-source or entry-level automation tools like Ansible or free-tier solutions to detect misconfigurations but does not require a reporting mechanism. Add reporting requirement to this enhancement.
8	Dr. Rich Osolease / RGB-PS LLC	Technical	22	819	Smaller organizations with limited IT staff may find dual authorization requirements burdensome and inefficient.	Enhancement 03.04.05E implies a need to establish a manual review process for critical system changes, leveraging simple documentation workflows or approval emails may not have technical dual authorization capabilities. The changed process should be allowed to count for the first level of approval.
9	Dr. Rich Osolease / RGB-PS LLC	Technical	36	1241	Advanced threat assessment frameworks are often beyond the capacity of small businesses due to high costs and expertise needs.	Enhancement 03.11.01E implies use of comprehensive risk assessment tools or templates provided by federal agencies like NIST to assess threats within operational constraints.
10	Dr. Rich Osolease / RGB-PS LLC	Technical	66	2231	Small businesses may lack the resources to conduct thorough supply chain risk assessments or monitoring.	Enhancement 03.16.01E implies mandatory collaboration with vendors to request security compliance certifications and use Federal available checklists to evaluate supply chain risks. Non-Federal should be able to meet Federal agency define mission-essential services requiring trust worthiness. The federal organization should originate the requirement.