By William Noble (wnoble2005@gmail.com) via xnetd.com

NIST 800-171 control 3.7.6 requires organizations to supervise maintenance personnel who lack full access permissions. This reduces the risk of unauthorized access and data breaches by ensuring only authorized individuals can perform maintenance. It also holds personnel accountable through supervision and creates an audit trail for tracking activities. Implementation involves defining authorized personnel and their access levels, approving and monitoring maintenance, and regularly reviewing and updating access controls.

1. Establish a Clear Authorization Process:
    a. Develop a documented process for authorizing individuals and organizations to perform maintenance on your systems.
    b. Define roles and responsibilities for authorizing individuals, including conducting background checks and assessing potential security risks.
    c. Maintain a list of authorized individuals and organizations with their specific access levels and maintenance scopes.
2. Categorize Maintenance Needs:
    a. Classify maintenance activities based on their complexity, sensitivity, and potential impact on the system.
    b. This helps determine the level of supervision and access control required for each type of maintenance.
3. Implement Least Privilege for Authorized Personnel:
    a. Grant authorized personnel the minimum level of access needed to perform their specific maintenance tasks.
    b. This minimizes the potential damage caused by accidental or malicious actions.
4. Grant Temporary Access (if necessary):
    a. For situations requiring immediate maintenance by personnel without pre-existing authorization, consider issuing temporary credentials with limited privileges and strict expiration times.
    b. Evaluate the necessity of temporary access beforehand and conduct risk assessments for each instance.
5. Implement Rigorous Supervision:
    a. Designate authorized personnel with the appropriate technical expertise and security awareness to supervise un-authorized maintenance activities.
    b. Supervisors should monitor the activity closely, ensuring adherence to established procedures and preventing unauthorized access or actions.
    c. This can involve observing the maintenance process, reviewing log files in real-time, or using remote monitoring tools.
6. Document and Audit:
    a. Document all maintenance activities conducted by unauthorized personnel, including the individual's name, organization, scope of work, supervisor assigned, and duration of access.
    b. Regularly audit these records to ensure compliance with procedures and identify potential anomalies.
7. Train and Educate:

    a. Train authorized personnel responsible for supervision on their roles and responsibilities, including identifying suspicious activity and escalation procedures.
    b. Educate unauthorized maintenance personnel on security policies and acceptable conduct while performing their tasks.
8. Leverage Technological Controls:
    a. Implement additional controls like two-factor authentication, privileged access management tools, and activity logging to further restrict unauthorized access and enhance auditability.
9. Continuously Improve:
    a. Regularly review and update your control implementation based on lessons learned, emerging threats, and changes in your organizational needs.